Cisco Security Cloud Control

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Security Cloud Control (the "Service"). The Service is a cloud-based security 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 Security Clound Control (formerly known as Security Cloud Control and Security Cloud Sign-On and Cisco Security Provisioning and Administration) 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.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Security Cloud Control is Cisco's unified, cloud-native security management interface for the Cisco Security Cloud. It simplifies and strengthens defenses by centralizing security solutions into a single, cohesive interface.

The Service is Cisco's secure identity solution used by various Cisco security and networking products. The Service is used as a single sign-on (SSO) across products, and operates as the native Identity Provider (IdP) or delegated IdP across selected Cisco products. It provides robust regulatory compliance, resilience, performance, and strong security through adaptive multi-factor authentication (MFA) powered by Cisco Duo ("Duo"). Customers also have the option to use the single sign-on provider of their choice.

The Service also enables delegated authentication through Cisco.com and Microsoft Azure. If a customer uses delegated authentication through Microsoft Azure, the customer's Microsoft Azure administrator determines, through the Microsoft Azure configuration, whether certain data listed below under "User Registration Information" is shared with The Service. Please refer to Microsoft's privacy policies for information regarding the processing of personal data by Microsoft Azure.

For more information about the Service, visit here.

2. Personal Data Processing

For the customers who use the Service, the table below lists the personal data used by this feature to carry out its function and describes why the Service processes that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Registration Information	• Email address • Password • Name • User information included in your directory if synced (e.g., name, username, display name, email, GroupName) • Organization • Title and/or role • Country • Business phone number • Information of Product Subscription contact (e.g. name, email)	• Account creation • Identity authentication • Provide the service • Customer relationship management (e.g., transactional communication) • Billing

	• Multi Factor Authentication information (e.g., phone number, email, device)	
Host & Usage Information	• User name • User activity (e.g. signed on or signed off specific app or product) • Geo Location – country/city based on IP address of device • ISP and IP Address • Browser and OS • Timestamp of User activity • API logs (e.g., email addresses, source IP, name and phone number) • Access logs (e.g., authentication methods, times) • Authentication tokens • Cookies • Device information	• Authentication • Audit trail • Adaptive MFA • Provide the service • Diagnose technical issues • Understand how the Service is used • Product improvement
Product Data[1] **(not stored)**	• Personal Data listed in your product's applicable Product Data Sheet available to view or to take action on through the Service.	• Deliver the Service

Note that all Cisco Security Provisioning and Administration accounts require Multi Factor Authentication (MFA) with Duo, but customers have the option to configure Google Authenticator (or any RFC 6238-compliant Time-based One-Time Password generator) as an alternative MFA. Please see the Duo privacy data sheet here for information on how your data is processed by Duo for the MFA function. Please see Google's privacy policies for information regarding the processing of personal data by Google.

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the account information provided by 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 Service Delivery Privacy Data Sheet.

You may access the Cisco AI Assistant through the Service. The Cisco AI Assistant provides actionable guidance across products, simplifying policy management for products such as Secure Firewall and Secure Access. Customers can also utilize natural language querying for documentation across various Cisco products. For information about how the Cisco AI Assistant processes your data, please see the AI Assistant Privacy Data Sheet.

3. Cross-Border Transfers

The Service leverages the third party cloud hosting providers shown below.

Data Center Locations
United States (AWS)

[1] Security Cloud Control allows your to view your data from certain active Cisco products ("Product Data") and take certain actions (e.g., view reports, make configuration changes). This data is processed real time to provide the Service but is not stored by Security Cloud Control. For information on how your Product Data is processed by the corresponding product, please see the appropriate Privacy Data Sheet here.

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

5. Access Control

The table below lists the personal data used by the Service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Registration Information	Customer	Users can modify personal information detailed in Section 2, as part of self-registration and manage users ability to reset passwords.
	Cisco	Maintain audit trail, investigate security threats; troubleshooting.
	Okta	Troubleshooting and support for solution problems; investigate security threats.
Host & Usage Information	Cisco	Maintain audit trail, investigate security threats; troubleshooting.
	Okta	Troubleshooting and support for solution problems; investigate security threats.
Product Data	Cisco	Provide the Service
	Customer	View reports and take product specific actions

6. Data Portability

The following personal data is made availableUser Registration Information. The availability of the data is subject to the deletion and retention policies described in Section 7 below.

7. Data Deletion & Retention

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

Type of Personal Data	Retention Period	Reason for Retention
User Registration Information	Upon termination of applicable Service subscription or by opening a Cisco TAC case.	Since the Service is used across various Cisco products, User Registration Information is maintained until Customer requests deletion via a Cisco TAC service request.
Host & Usage Information	12-months.	Provide the Service
Product Data	Not Stored	N/A

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
User Registration Information	Data is encrypted in transit and at rest
Host & Usage Information	Data is encrypted in transit and at rest
Product Data	Data is encrypted in transit (not stored by the Service)

9. 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 provided to you by Cisco. The current list of sub-processors is set out 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
Okta	• User Registration Information • Host & Usage Information	Okta Identity Cloud is hosted in AWS West, and makes use of servers and storage in AWS to implement Okta Identity Cloud.	United States
AWS	• User Registration Information • Host & Usage Information	AWS cloud infrastructure is used to host the Service.	United States
DataDog	• User Registration Information • Host & Usage Information	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics.	United States

Microsoft Azure	• User Registration Information	If Customer chooses to leverage Microsoft Azure, Cisco will process (but not store) User Registration Information with Microsoft Azure.	United States
Amplitude	• Host & Usage Information	Analytics	United States

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), 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 about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Laws

The Security and 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.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

Additionally, a current list of Okta certifications can be found at https://www.okta.com/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 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.

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.

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