Cisco Smart Net Total Care

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Smart Net Total Care ("SmartNet").

SmartNet is a service made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from SmartNet 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 SmartNet in order to provide its functionality.

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

1. Overview

SmartNet helps reduce network downtime with fast, expert technical support and flexible hardware coverage provided by the Cisco Technical Assistance Center (TAC). It also offers integrated smart capabilities, providing current information about your installed base of Cisco products, contracts, and security alerts to enhance the efficiency of your support workflows. The TAC is staffed by Cisco experts and is accessible 24 hours a day, 365 days per year. Technical services available through the TAC are backed by advance hardware replacement options and fast response time, including 2 - hour, 4 - hour, and next - business - day options (where available). Online self-help tools include our extensive knowledge library, software downloads, and support tools designed to help you resolve network issues quickly without opening a case.

Smart capabilities are delivered through the SmartNet portal, providing actionable information and automation to support your Cisco products. Customizable screens show you up-to-date information about the service coverage, product lifecycles, and security and product alerts that apply to your network. The portal also provides interactive workflows that simplify support management processes. These foundational technical services and smart capabilities can help you resolve problems more quickly, mitigate risk, and improve operational efficiency.

For a more detailed description of the SmartNet Service, please see: https://www.cisco.com/c/en/us/services/technical/smart-net-total-care.html

2. Personal Data Processing

This Privacy Data Sheet covers all aspects of the SmartNet service including Smart capabilities. Smart capabilities, which are an optional set of features available to all SmartNet contract holders, allow Customers to opt into sending device data to Cisco. If a Customer opts not to utilize Smart capabilities, then the only personal data that will be processed is for TAC Assistance. The tools are used to discover, collect and upload device data to Cisco are Cisco's Common Services Platform Collector (CSPC) and other collection methods. These other collection methods are *optional alternatives* and include tools from SolarWinds and Netformx, as well as Comma Separated Value (CSV) uploads. Collected device data are enriched with Cisco supplied data pertaining to device lifecycle, support coverage, and impacting alert data. Customers, Partners and users may view and export their data for their business needs. Cisco requires that Customers and users register in the SmartNet Portal to access Smart capabilities, as a result some personal data may be collected. If you are a SmartNet Portal user and your employer is the Customer that purchased the SmartNet Service, all exported information described in this Privacy Data Sheet is then subject to your employer's applicable policies regarding retention, monitoring, deletion, and export of information associated with the Service.

The table below lists the personal data processed by SmartNet to provide its services and describes why the data is processed.

Table 1 SmartNet Portal

Personal Data Category	Types of Personal Data	Purpose of Processing
SmartNet Portal Administration Information	• Cisco User Name (CCO ID) • Email Address • Contract Number • Serial Number	We use this information to validate entitlement to and remote access to SmartNetPortal and CSPC software.

Table 2 Cisco Common Service Platform Collector (CSPC) and other device data collection methods (optional Solarwinds, Netformx, CSV uploads)

Personal Data Category	Types of Personal Data	Purpose of Processing
Host and usage information	Cisco does not intentionally collect or process personal data via CSPC. Outside of CSPC, we instruct Customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be collected and processed from CSPC or other collection methods for the purpose of providing support: • Device Configuration (e.g., running config and startup config, SNMP Strings (masked), Interface description) • Command Line Interface (CLI) (show commands, e.g., show version)	We use Host and Usage Information to: • Understand how the Service is used • Diagnose technical issues • Conduct analysis in aggregate form to improve the technical performance of the Service • Respond to Customer Support requests • Report enriched information back to authorized users

Table 3 Technical Support Assistance (TAC)

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• Full Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) (CCO ID)	• We use TAC Support Information to: • Provide remote access support • Review quality of the support service • Perform analysis of the service solution

SmartNet support is delivered through Cisco's TAC, which is a global organization that provides around-the-clock, technical support services online and over the phone. TAC offers Customer support for SmartNet using a global follow-the-sun support model. Our teams support thousands of service requests every day, as well as supply hardware support, repair, and replacement from one of our 1,100 hardware depots.

For additional information related to Cisco TAC delivery, please visit the following privacy data sheet. Cisco TAC Delivery: Essential Technical Support.

3. Data Center Locations

Cisco uses its own data centers as well as third-party infrastructure providers to deliver the service globally.

Cisco Data Center Locations
Richardson, Texas, USA
Allen, Texas, USA
Research Triangle Park, North Carolina, USA

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

Cisco Smart service capabilities require that the Customer assign an employee Designation Administrator (DA) to manage user access to the reporting portal and other reporting mechanisms like Application Programable Interfaces (APIs). The table below lists the personal data used by this Service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
Registration Information	**Customers**: • Administration Management (CSAM) tool • Administrator through the SmartNet Portal after DA creation	Modify, add, delete customer and partner administrators and users
	End-Users: • Designated Administrator (DA) through the Cisco Services Administration Management (CSAM) tool	Modify, add, delete Customer and partner administrators and users
	Cisco: • Cisco employees supporting service offering	Support and improve the Service by the SmartNet Support and Development teams
	Partners: • Administrator through the SmartNet Portal after MSP (Managed Services Providers) DA creation and customer role assignment	Modify, add, delete customer and partner administrators and users

Collected and Reported data	**Customers**: • Customer Users and Administrators	Obtain reported information and manage other users
	End-Users: • Customer Users and Administrators	Obtain reported information and manage other users
	Cisco: • Cisco employees supporting service offering	Support and improve the Service by the SmartNet Support and Development teams
	Partners: • Customer Users and Administrators	Obtain reported information and manage other users
Usage	**Cisco**	Cisco analyzes collected data and usage data to improve Services and products
	Partners	Manage business information on behalf of the Customer, with the Customer's authorization

6. Data Portability

Cisco Smart service capabilities allow customers and authorized users to export reported data via the SmartNet Portal. Customers may also access these reports by using APIs or by exporting the data through Comma Separated Value (CSV) format. Partners who have been authorized by their Customers may also view, export or use APIs to obtain collected and enriched data.

7. Data Deletion and Retention

Type of Personal Data	Retention Period	Reason for Retention
Customers collected Inventories	2 Years, Customer may delete inventories anytime, by executing steps in the Smart Net Total Care portal users guide	Data is retained for 2 years to provide delivery of the Smart Net Total Care service offering.
User Registration data	Customers may delete user registration data in the Smart Net Total Care portal.	Data is retained for 2 years to provide delivery of the Smart Net Total Care service offering.
Personal data	Individuals may request deletion of personal data retained by Cisco TAC by submitting a request via privacy portal and unless the personal data are required to be retained for Cisco's legitimate business interests or otherwise under applicablelaw, they will be deleted within 30 days of the requested action.	Data is retained for 2 years to provide delivery of the Smart Net Total Care service offering.

8. Personal Data Security

Cisco's Customer Experience Organization that provides SmartNet is ISO 27001 certified and in accordance with those standards adopts technical and organization security measures to protect your personal data from unauthorized access use or disclosure as required by law.

Personal Data Category	Type of Encryption
Registration data	Passwords are encrypted
SmartNet Smart Capabilities collected data	Encrpyted in transit; documents containing customer data are encrypted 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
Khoros	CCO ID profileinformation	Delivery support on behalf of Cisco Systems, Inc. Community platform for Cisco Customers and Partners https://community.cisco.com/t5/smart-net-total-care/ct-p/4891-smart-net-total-care	USA
Snowflake	None	Hosting/database for SNTC Collected data	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), 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 Requirements

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

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security. Cisco's Customer Experience organization that provides SmartNet has received the following certifications:

- ISO 27001

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:

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	**EMEAR 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.