# 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 ("Smart Net").

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

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

## 1. Overview

Smart Net helps reduce network downtime with fast, expert technical support and flexible hardware coverage provided by the Cisco Technical Assistance Center (TAC). It 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 using a global follow-the-sun support model. 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 Smart Net 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.

For a more detailed description of the Smart Net Service, please see: Smart Net Total Care At-A-Glance.

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

**Please note Cisco is in the process of decommissioning the Smart Net Portal. The Portal will be replaced with Cisco Customer Experience (CX) Cloud referred to as "CX Cloud." For Customers using the Cisco CX Cloud portal, refer to the Cisco CX Cloud table information (in addition to the other tables). For Customers using the Smart Net Portal, refer to the Smart Net Portal table information (in addition to the other tables).**

## 2. Personal Data Processing

This Privacy Data Sheet covers all aspects of the Smart Net service including Smart capabilities. Smart capabilities, which are an optional set of features available to all Smart Net 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 that 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 Smart Net Portal to access Smart capabilities, and as a result some personal data may be collected. If you are a Smart Net Portal user and your employer is the Customer that purchased the Smart Net 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 what personal data is processed by Smart Net to deliver the offer Smart Net, including the business purpose of the data element collected.

### Cisco CX Cloud

| Personal Data Category | Types of Personal Data | Purpose of Processing |
|---|---|---|
| Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet |

### Smart Net Portal

| Personal Data Category | Types of Personal Data | Purpose of Processing |
|---|---|---|
| **Smart Net Portal Administration Information** | <ul><li>Cisco User Name (CCO ID)</li><li>Email Address</li><li>Contract Number</li><li>Serial Number</li></ul> | <ul><li>Validate entitlement to and remote access to Smart Net Portal and CSPC software</li><li>Manage Customer Account and Services Activation</li><li>Authenticate and Authorize access to Smart Net portal</li><li>Portal login count</li><li>Audit trailing</li></ul> |

### 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.<br><br>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.<br><br>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:<br><ul><li>Device Configuration (e.g., running config and startup config, SNMP Strings (masked), Interface description)</li></ul> | <ul><li>Understand how the Service is used</li><li>Diagnose technical issues</li><li>Conduct analysis in aggregate form to improve the technical performance of the Service</li><li>Respond to Customer Support requests</li><li>Report enriched information back to authorized users</li></ul> |

| | | |
|---|---|---|
| | • Command Line Interface (CLI) (show commands, e.g., show version) | |

## Technical Support Assistance (TAC)

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

# 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 |
|---|
| **Allen, Texas, USA** |
| **Richardson, Texas, USA** |
| **RTP Campus, North Carolina, USA** |
| **Amsterdam, Netherlands** |

| Infrastructure Provider |
|---|
| **AWS – Oregon, USA** |
| **AWS – Frankfurt, Germany** |
| **AWS – Sydney, Australia** |

| |
|---|
| **AWS – Virginia, USA** |
| **SalesForce.com Data Center – Washington DC, USA** |
| **Cisco Managed Snowflake AWS – US EAST 1** |
| **MapBox - USA** |

| Subcontractors | Subcontractor Datacenter Locations |
|---|---|
| **SalesForce.com** | Washington, D.C., USA |
| **Snowflake** | Virginia, USA |
| **Khoros** | Oregon, USA and Ireland |
| **Okta, Inc.** | Oregon, USA |

**Theater to AWS Region Mapping in CX Cloud**

| Theater/Location | AWS Region |
|---|---|
| **Americas** | US (Oregon) |
| **Asia Pacific, Japan** | Asia Pacific (Sydney) |
| **Europe, Middle East, Africa** | EU (Frankfort) |

# 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

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). In the event that the Customer does not assign an employee DA, Cisco may assign roles with customer approval. The table below lists the personal data used by this Service, who can access that data, and why.

Partners who have been authorized by their Customers may also view, export or use APIs to obtain collected and enriched data.

**Cisco CX Cloud**

| Personal Data Category | Who has Access | Purpose of the Access |
|---|---|---|
| Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet |

**Smart Net Portal**

| Personal Data Category | Who has Access | Purpose of the Access |
|---|---|---|
| **Smart Net Portal Administration Information** | Customers:<br>• Administration Management (CSAM) tool<br>• Administrator through the SmartNet Portal after DA creation | Modify, add, delete customer and partner administrators and users |
| | End-Users:<br>• Designated Administrator (DA) through the Cisco Services Administration Management (CSAM) tool | Modify, add, delete Customer and partner administrators and users |
| | Cisco:<br>• Cisco employees supporting service offering | Support and improve the Service by the SmartNet Support and Development teams |
| | Partners:<br>• 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 |

**Cisco Common Service Platform Collector (CSPC) and other device data collection methods (optional Solarwinds, Netformx, CSV upload**

| Personal Data Category | Who has Access | Purpose of the Access |
|---|---|---|
| **Collected and Reported data** | Customers:<br>Customer Users and Administrators | Obtain reported information and manage other users |
| | End-Users:<br>Customer Users and Administrators | Obtain reported information and manage other users |
| | Cisco:<br>Cisco employees supporting service offering | Support and improve the Service by the SmartNet Support and Development teams |
| | Partners:<br>Customer Users and Administrators | Obtain reported information and manage other users |
| **Host and Usage Data** | 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 Retention

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

| Type of Personal Data | Retention Period | Reason for Retention |
|---|---|---|
| **Host and Usage 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. |
| **TAC Support Information** | Please refer to the Cisco TAC Delivery Privacy Data Sheet: Cisco TAC Service Delivery. | Please refer to the Cisco TAC Delivery Privacy Data Sheet: Cisco TAC Service Delivery. |

**Cisco CX Cloud**

| Type of Personal Data | Retention Period | Reason for Retention |
|---|---|---|
| **User Account and Registration Information** | Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet |

**Smart Net Total Care Portal**

| Type of Personal Data | Retention Period | Reason for Retention |
|---|---|---|
| **Smart Net Portal Administration Information** | 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. |

# 7. Personal Data Security

Cisco's Customer Experience Organization that provides Smart Net is ISO 27001:2013 certified and in accordance with those standards adopts appropriate technical and organizational measures to protect your personal data from unauthorized access use or disclosure as required by law.  These technical and organizational measures include the following:

| Personal Data Category | Security Controls and Measures |
|---|---|
| **Host and Usage Information** | Encrpyted in transit; documents containing customer data are encrypted at rest |
| **TAC Support Information** | Please refer to the Cisco TAC Delivery Privacy Data Sheet: Cisco TAC Service Delivery. |

**Cisco CX Cloud**

| Personal Data Category | Security Controls and Measures |
|---|---|
| **CX Cloud Administration Information** | Refer to the CX Cloud Privacy Data Sheet |

**Smart Net Total Care Portal**

| Personal Data Category | Security Controls and Measures |
|---|---|
| **Smart Net Portal Administration Information** | Passwords are encrypted in transit and at rest |

# 8. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below.  Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

**Smart Net Portal**

| Sub-processor | Personal Data | Service Type | Location of Data Center |
|---|---|---|---|
| **Khoros** | CCO ID profile Information | Delivery support on behalf of Cisco Systems, Inc. Community platform for Cisco Customers and Partners Smart Net Total Care Community | USA |
| **Salesforce.com (USA)** | User Account and Registration Information | Trusted Support. Third party cloud hosting service for supporting the case management system. | Washington, D.C., USA. For more information on Salesforce.com data center locations please visit Salesforce.com here |
| **Okta, Inc.** | User Account and Registration Information | Third party identity management services handling authentication | US West and Backup (DR) Region US East |
| **Snowflake, Inc.** | Asset Management Data | Leveraging data warehousing services as means to aggregate corporate sales data (hardware assets, software assets, subscriptions, etc.) | AWS data centers in the United States. |

**Cisco CX Cloud**

| Sub-processor | Personal Data | Service Type | Location of Data Center |
|---|---|---|---|
| Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet | Refer to the CX Cloud Privacy Data Sheet |

# 9. Information Security Incident Management

**Breach and Incident Notification Processes**

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

# 10. Certifications and Compliance with Privacy Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The service is built with security and privacy in mind and is designed so that it can be used by Cisco Customers in a manner consistent with global security and privacy requirements.

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

- ISO 27001:2013

If you are using CX Cloud, please refer to the CX Cloud Privacy Data Sheet.

# 11. 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.

Cisco Smart service capabilities allow customers and authorized users to export reported data via the Smart Net Portal. Customers may also access these reports by using APIs or by exporting the data through Comma Separated Value (CSV) format.

If you are using CX Cloud, please refer to the CX Cloud Privacy Data Sheet.

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

# 12. 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.