# Smart Software Licensing Tools and Smart Account Management

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Smart Software Licensing tools and Smart Account Management.

Smart Software Licensing tools and Smart Account Management is a set of cloud-based licensing software made available by Cisco to companies or persons who acquire Cisco products for use by their authorized users.

Cisco will process personal data from Smart Software Licensing tools and Smart Account Management 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 Software Licensing tools and Smart Account Management in order to provide its functionality.

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

## 1. Overview

Smart Software Licensing and Smart Accounts is a new, time-saving method of customer software license asset management. Through an account on the Cisco.com website, it lets you view and control access to all of your Cisco software licenses and entitlements across your organization. Before Smart Accounts, visibility to entitlements required individual Cisco.com identification, which restricted license management and reporting capabilities across the enterprise.

After creation of a Smart Account, customers can create mutliple virtual accounts under their smart accounts, then associate licenses with those virtual accounts. Virtual accounts can be created to reflect company organization, geography, budgeting or other structure.

Smart Accounts span multiple tools including CSSM, LRP, CCW and Software Central. The following describes the capabilities that are part of the smart software licensing and smart account management:

1. Software Central (https://software.cisco.com/): Customer facing portal to manage downloads and upgrade products, order, access to EULA tools, Smart Software Licensing tools and Smart Account Management.
2. License Registration Portal (LRP): Primary location for customers to access and manage/consume PAKs or other legacy licenses.
3. Cisco Commerce Workspace (CCW): Primary location for customers to procure Cisco products.

For more information about Smart Software Licensing tools and Smart Account Management, visit https://software.cisco.com/

## 2. Personal Data Processing

The table below lists the personal data processed by Smart Software Licensing tools and Smart Account Management to provide its services and describes why the data is processed.

**Smart Account Management:**

| Personal Data Category | Type of Personal Data | Purpose of Processing |
|---|---|---|

| | | |
|---|---|---|
| **Customer Smart Account Details** | • First / Last Name<br>• Email Address<br>• CCO User ID<br>• Role<br>• Company locations<br>• Other account related attributes like Status, domain | • Create and manage the account |

**Smart Licensing:**

| Personal Data Category | Type of Personal Data | Purpose of Processing |
|---|---|---|
| **Customer Account Details** | • Email Address<br>• CCO User ID | • Associate assets with specific customer/account<br>• User action logs<br>• Event notifications |
| **Order Information** | • Order Number<br>• Subscription ID | • Traceability of orders<br>• Make sure account/customers have right level of access |
| **Device information** | • IP Address<br>• Hostname (can be opted out) | • Manage licenses used by the device |

# 3. Data Center Locations

Cisco uses its own data centers to deliver the service globally. Following data centers are used for Smart Software Licensing tools and Smart Account Management.

| Cisco Data Center Locations |
|---|
| Allen, Texas USA |
| Richardson, 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
- 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 Smart Software Licensing tools and Smart Account Management to carry out the service, who can access that data, and why.

**Smart Account Management:**

| Personal Data Category | Who has Access | Purpose of the Access |
|---|---|---|
| **Customer Smart Account Details** | • Cisco Admin, Cisco Support<br>• Customer Admin<br>• End user | • Create and manage the account |

**Smart Licensing:**

| Personal Data Category | Who has Access | Purpose of the Access |
|---|---|---|
| **Customer Account Details** | • Cisco Admin, Cisco Support<br>• Customer Admin<br>• End user | • Associate assets with specific customer/account<br>• View user action logs |
| **Order Information** | • Cisco Admin, Cisco Support<br>• Customer Admin<br>• End user | • Traceability of orders |
| **Device information** | • Cisco Admin, Cisco Support<br>• Customer Admin<br>• End user | • View and manage licenses used by the device |

# 6. Data Portability

Customers (administrator or user) can export the data they have access to, they can do so by using the reporting capability available by the smart account platform. Any additional support needed for data protection you can contact privacy@cisco.com or opening a TAC support request. Cisco will carry out the necessary due diligence to validate the request from an access control point of view.

# 7. Data Deletion and Retention

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

**Smart Account Management:**

| Personal Data Category | Retention Period | Reason for Retention |
|---|---|---|
| **Customer Smart Account Details** | • Activity logs and events are deleted after 2 years<br>• Deactivated transaction records are retained in the backend but not shown on UI | • Audit purpose<br>• To avoid creating duplicates |

**Smart Licensing:**

| Personal Data Category | Retention Period | Reason for Retention |
|---|---|---|
| **Customer Account Details** | • Activity logs and events are deleted after 2 years<br>• Deactivated transaction records are retained in the backend but not shown on UI | • Audit purpose<br>• To avoid creating duplicates |

| | | |
|---|---|---|
| **Order Information** | • Activity logs and events are deleted after 2 years<br>• Deactivated transaction records are retained in the backend but not shown on UI | • Audit purpose<br>• To avoid creating duplicates |
| **Device information** | • Activity logs and events are deleted after 2 years<br>• Deactivated transaction records are retained in the backend but not shown on UI | • Audit purpose<br>• To avoid creating duplicates |

# 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.

Smart Software Licensing and Smart Accounts adopt technical and organizational security measures as required by law and in accordance with industry standards that are designed to protect personal data from unauthorized access, use or disclosure. In addition, the data is hosted at Cisco data centers in USA and has undergone data security and vulnerability reviews to ensure best practices and controls are in place.

**Smart Account Management:**

| Personal Data Category | Security Controls and Measures |
|---|---|
| **Customer Smart Account Details** | Encrypted in transit, but not at rest (see above for how we protect this data at rest) |

**Smart Licensing:**

| Personal Data Category | Security Controls and Measures |
|---|---|
| **Customer Account Details** | Encrypted in transit, but not at rest (see above for how we protect this data at rest) |
| **Order Information** | Encrypted in transit, but not at rest (see above for how we protect this data at rest) |
| **Device information** | Encrypted in transit, but not at rest (see above for how we protect this data at rest) |

# 9. Sub-processors

Smart Software Licensing and Smart Accounts does not use sub-processors to provide its services.

# 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 & 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.

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 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:

<table>
<tr><td colspan="3">Chief Privacy Officer<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer<br>Cisco Systems, Inc.<br>170 W. Tasman Drive<br>San Jose, CA 95134<br>UNITED STATES</td><td>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</td><td>EMEA Privacy Officer<br>Cisco Systems, Inc.<br>Haarlerbergweg 13-19, 1101 CH<br>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. 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.