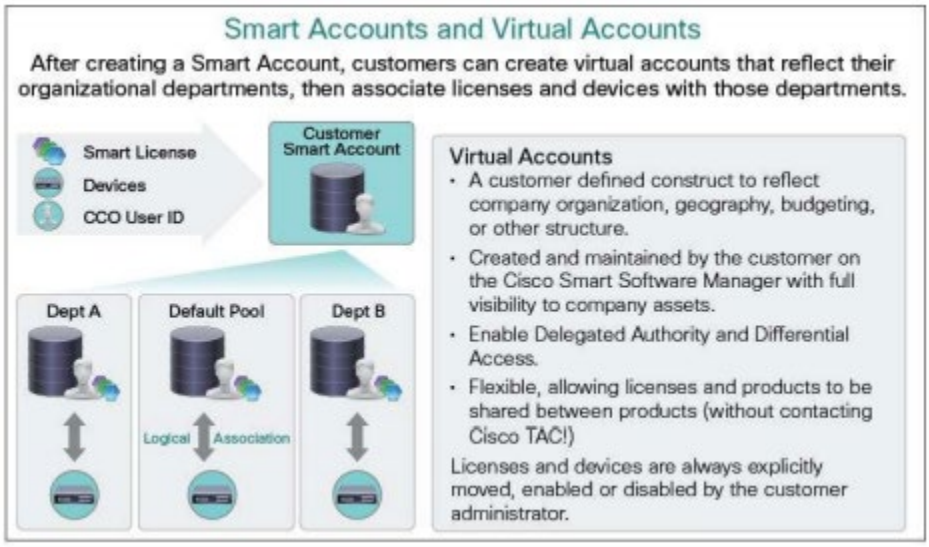
Smart Software Licensing Tools and Smart Account Management

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

1. Overview of Cisco Smart Accounts Capabilities

Cisco 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 (Figure 1). Before Smart Accounts, visibility to entitlements required individual Cisco.com identification, which restricted license management and reporting capabilities across the enterprise.



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 (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.
3. License Registration Portal (LRP): Primary location for customers to access and manage/consume PAKs or other legacy licenses.
4. Cisco Commerce Workspace (CCW): Primary location for customers to procure Cisco products.

2. Personal Data Processing

The table below lists the personal data used by Cisco Smart Accounts to carry out the services and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Customer Contact Details	• First / Last Name • Email Address • CCO User ID • Role	• Create and manage the account
Customer Account Details	N/A	• Associate assets with specific customer/account
Order Information	N/A	• Traceability of orders • Make sure account/customers have right level of access
Device information	• IP Address • Hostname (can be opted out)	• Traceability of orders • Make sure account/customers have right level of access

3. Data Ingest Process

Cisco uses the Cisco Smart Software Manager (CSSM), which is a Software inventory management system that provides information about software ownership and usage. This also includes Smart Software Manager satellite (CSSMs) which collects software inventory locally and transmits the information to CSSM.

4. Cross-Border Transfers

The data is hosted and managed at Cisco data center in California, USA. The data can be collected/generated at local sites but the production instance is hosted at the Cisco data center in San Jose, California. Cisco IT maintains the governance related to replication and internal Cisco personnel access to the data. All the replication sites are within the US.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

5. Access Control

The access methods are created according to the principle of least privileged access. The following roles are used to grant access:

- Smart Account User - Manages assets within all Virtual Accounts but cannot add or delete Virtual Accounts or manage user access.

- Smart Account Administrator - Manages all aspects of the Smart Account and its Virtual Accounts including Users.

- Smart Account Approver – They can only approve license agreement on behalf of the account owner. Includes no User or Administrator privileges such as adding roles and associating entitlements and licenses.

- Virtual Account is a default sub account/container to segregate entitlements and license for customers. Customers govern the virtual accounts. Customer entitlements and assets are defined and segregated at the level of virtual accounts.

- Virtual Account User – Can do everything for entitlement management but not assign roles.
- Virtual Account Administrator – Can assign roles to other users; scope is contained to virtual accounts.

Smart Account Administrator contact information is only shared with employees of the same organization, not with an outside party beyond Cisco (unless requested by customer). If a partner does not have access to a smart account and would like to gain access or communicate to a Smart Account administrator, they may use the Smart Account Request Access tool found on software.cisco.com. A message is then sent to all Smart Account administrators without divulging their names to the requestor.

CSSM Satellite Accounts: These accounts provide ability for customers to integrate access control using their enterprise identity and access federation. This is not based on CCO ID authentication and uses local authentication based on customer's identity and access management.

Access to Personal Data is controlled as follows:

- Cisco IT maintains the governance related to replication and internal Cisco personnel access to the data.

- In accordance to Cisco internal data classification, governance and policies, Cisco users are subject to periodic revalidation of their access to the smart account platform.

- Customers are allowed to share their Smart Account Data with anybody they choose, but any additional 3rd party must be explicitly added, and Cisco will not share the information with a 3rd party unless the customer explicitly requests it.

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 & Retention

User level information is deactivated immediately after the smart account administrator removes a user from the specific smart account. The user level information (post de-activation) and user event logs are governed by standard Cisco data retention and deletion practices.

Smart account names are not deleted by Cisco as the name is associated to customer specific assets and entitlements. As the customer owns this association, Cisco doesn't delete this data.

8. Personal Data Security

Smart Software Licensing and Smart Accounts adopts 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 a Cisco data center in California, USA and has undergone data security and vulnerability reviews to ensure best practices and controls are in place.

Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Type of Encryption
Customer Contact Details	Encrypted in transit, but not at rest (see above for how we protect this data at rest)
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. Third Party Service Providers (Sub-processors)

Cisco performs the Service without sending Registration Information, Host and Usage Information, and User-Generated Information to any third-party service providers.

10. Information Security Incident Management

Breach and Incident Notification Processes
The Data Protection & Privacy 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. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Services has received the following certifications:

- ISO 27001

12. General Information and GDPR FAQ

How does Smart Account enable a Customer to manage and protect their assets & entitlements?
Cisco Smart Accounts is a new, time-saving method of customer managed 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 you set up a Smart Account, you have the flexibility to create sub accounts (virtual accounts) to help manage your licenses for departments, areas, or locations within your organization. Licenses can be pooled within virtual accounts as needed. Smart Accounts have role-based user access controls, which allow the delegation of authority to account administrators at the Smart Account level or at the virtual account level. In addition, you can manage partner visibility and management rights to your virtual or enterprise-level accounts.
https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/smart-software-manager-satellite/at-a-glance-c45-734361.pdf

Can there be more than one individual within an organization have access to licenses and entitlements in a Smart Account?
Yes. You may add as many Administrators or Users as you like to your Smart Account. Each User or Administrator can have access to either the entire Smart Account or individual Virtual Accounts (Smart Account Folders) as is appropriate. You may define additional users either at Smart Account setup or anytime by going to the 'Manage my Smart Account' application on software.cisco.com.

Do Partners see or have access to Customer's Smart Account post-delivery of entitlements?
Third parties such as Partners or System Integrators only have access to the Customer's Smart Account only if the customer provides them with access either to the entire Smart Account or just the Virtual Accounts (Smart Account folders) that the customer wants to share to the partner. Smart Accounts also makes it easy for a customer to provide the partner with complete access to their Smart Account if that is what they choose; simply add the partner contact to the authorized users list when initially setting up the Smart Account or by using the 'Manage my Smart Account' application on software.cisco.com.

If a customer purchased and delivered a bunch of licenses into their smart account from two different partners – can the partner see my total entitlements in my Smart Account?
Customer have the control to provide visibility. The customer may give both partners access to the entire Smart Account, or you can give each partner access only to a portion of it.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.