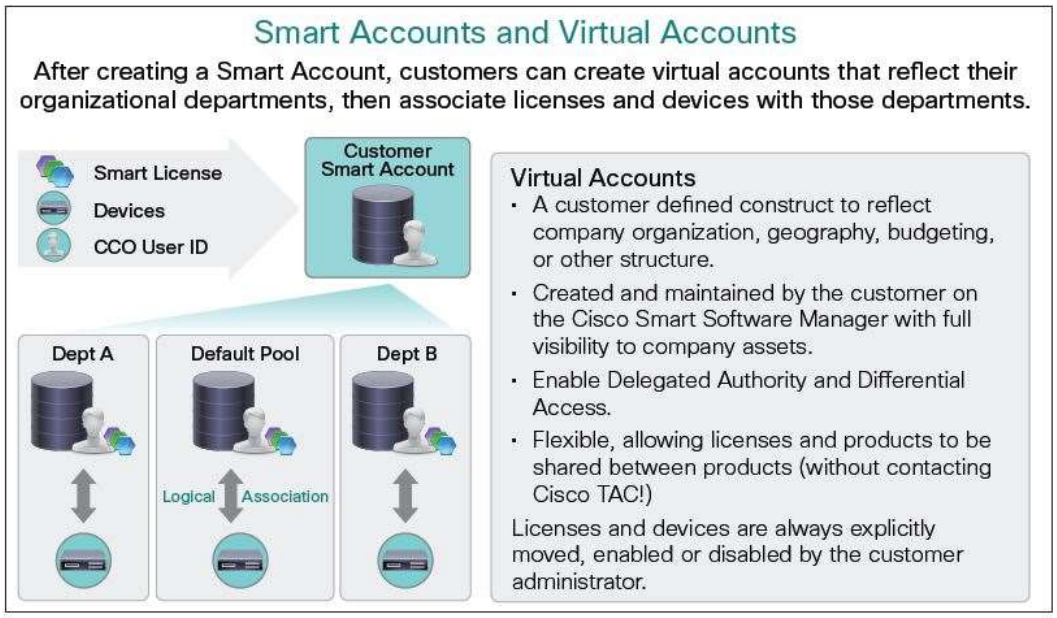
Smart Software Licensing tools and Smart Account Management Privacy DataSheet

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

1. Overview of 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. **Cisco Smart Software Manager (CSSM):** 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.
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

Smart software licensing and smart account management leverages the following data to provide the ability to have visibility and access control of licenses across the customers company:

Data Type	Personal Data Elements	Purpose of Processing
Customer Contact Details	First / Last Name, Email Address, CCO User ID, Role	Purpose of data collection is create and manage the account
Customer Account Details	NA	To associate assets with specific customer/accounts
Order Information	NA	Collected for tracebility of orders; to make sure account/customers have right level of access
Device information	IP Address, Hostname (can be opted out)	Collected for tracebility of orders to make sure account/customers have right level of access

3. 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.

4. Access control

The access methods are created according to the principle of least privileged access. The following roles are used to gramt 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 entilements and licenses.

Virtual Account is a default sub account/container to segregate entitlements and license for customers. Customers govern the virtual accounts. Customer entitlments and assets are defined and seggregated 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.

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 explicity added and Cisco will not share the information with a 3rd party unless the customer explicitly requests it.

5. Retention Period and Data Deletion

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.

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. 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 CA, 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.

Data Type	Type of Encryption
Customer Contact Details	Encrypted in transit, but not at rest (see below for how we protect this data at rest)
Customer Account Details	Encrypted in transit, but not at rest (see below for how we protect this data at rest)
Order Information	Encrypted in transit, but not at rest (see below for how we protect this data at rest)

Device information	Encrypted in transit, but not at rest (see below for how we protect this data at rest)

8. 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.

9. 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. Smart Software Licensing and Smart Accounts 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.

Smart Software Licensing and Smart Accounts leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- US-EU and Swiss-US Privacy Shields
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

10. Coporate Quality Compliance and Certifications

Cisco holds a Global ISO 9001 Certification and ISO 14001 Registration, managed by the Corporate Quality Compliance and Certifications program, which establishes and maintains policies that ensure quality management of processes and environmental responsibilities. Visit our Quality Certifications page to understand the scope of these compliance certifications and read more information.

11. 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.

12. Privacy and Data Protection 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?

3rd 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 expose to the partner. The choice is completely in the customers' hands! 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.

What is GDPR and who does it affect?

The European Union General Data Protection Regulation, or EU GDPR, became effective as of May 25, 2018, and affects organizations that process EU personal data. Aimed at protecting the fundamental right to privacy, the new regulations are broad, strict, and require adherence from organizations all over the world. Even for organizations not based in Europe, if an organization is offering goods or services to persons in

the EU or monitoring behavior of persons in the EU, such organization must comply with GDPR.

Will Smart Software Licensing and Smart Account management make an organization GDPR compliant?

No single product/application will make an organization GDPR compliant. GDPR is the legislative embodiment of privacy best practices and calls for transparency, fairness, and accountability when processing personal data. GDPR pushes the concepts of Privacy by Design and by Default: privacy and data protection have to be built-in and integrated in all data processing activities performed by the entity (the data controller) or by external organizations on its behalf (the data processor). This is about respecting individual rights, secure processes, and managing risk. Well-applied technology solutions can help underpin success. For example, Smart Software Licensing and Smart Account management can help the customer raise their security levels by helping them to understand what and where personal data is stored in the cloud and by alerting customers to suspicious user activity that might suggest an account compromise.

Does personal data need to remain in the EU or in any specific European Country?

No. People often assume that the EU GDPR requires data localization and that personal data must remain in the EU. GDPR provides that EU personal data should be processed in the EU unless you have approved mechanisms that allow for the international transfer of data. For example, Cisco has certified compliance with the EU-US and Swiss-US Privacy Shield which commits Cisco to a set of privacy principles and practices aligned to EU law when processing EU personal data in the US. The Shield framework has been deemed "adequate" by the European Commission – meaning EU personal data can flow to Shield certified companies and hence can flow to Smart Software Licensing and Smart Account management.

If necessary, Cisco can also execute EU Standard Contractual Clauses with the customer, which contractually binds Cisco to adhere to EU privacy standards. Use of Standard Contractual Clauses have been approved by the European Commission to allow transfers of EU personal data outside of the EU.

What is Cisco's stance on data privacy?

Cisco respects and is committed to protecting personal information. Our privacy statements reflect current global principles and standards on handling personal information: notice and choice of data use, data access and integrity, security, onward transfer and enforcement/oversight.

Cisco is certified under the EU-US and Swiss-US Privacy Shield frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, processing, and cross-border transfer of personal data from the EU and Switzerland. Cisco is also certified under the APEC Cross Border Privacy Rules system (www.cbprs.org) which has been endorsed by the 21 member economies of the Asia Pacific Economic Cooperation (APEC) organization as providing an appropriate baseline for privacy and data protection. To read Cisco's full privacy statement visit:
https://www.cisco.com/c/en/us/about/legal/privacy.html

What does the Smart Software Licensing and Smart Account management privacy and data security program entail?

Cisco takes a systematic approach to data protection, privacy, and security. We believe a comprehensive security and privacy program requires executive sponsorship and active involvement of cross-functional

stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization.

Cisco has established formal policies and supporting procedures concerning the privacy, security, review, and management of our products and services. The Cisco Chief Security and Trust Officer, Chief Privacy Officer (including EMEAR, APAC and Americas Privacy Officers), Chief Information Security Officer, and Global Data Protection & Privacy Counsel maintain overall responsibility for the program, which is evaluated on a regular basis. This helps ensure it is up to date and follows modern security standards and best practices, as well as compliance with applicable privacy regulations. The Cisco Security and Trust Organization's Information Security and Data Protection and Privacy programs include technical and organizational measures designed to help ensure physical and cyber security, data integrity, privacy, and transparency.

The Smart Software Licensing and Smart Account management is designed for top-tier security and data privacy, and follows industry-leading best practices for security and privacy. As set forth above, Smart Software Licensing and Smart Account management data centers are certified by various industry recognized standards. These data centers feature state of the art physical and cyber security and highly reliable designs.

You can view the following resources for more information:

· https://blogs.cisco.com/security/gdpr-cisco-and-you
· https://www.cisco.com/c/en/us/about/trust-center/privacy-podcast.html
· https://www.cisco.com/c/en/us/products/security/general-data-protection-regulation.html