Privacy Data Sheet

Cisco Secure Access China operated by Digital China Cloud Technology Limited

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Access China operated Digital China Cloud (“Secure Access China”).

Secure Access China is a cloud-based security solution operated by Digital China Cloud Technology Limited (“DCC”) to companies or persons who obtain a Secure Access China cloud service subscription. Secure Access China is provided by DCC based on the technology licensed to DCC by Cisco International Limited (“Cisco”). The service’s underlying technology is developed and maintained by Cisco and its affiliates, but the China service is operated and provided by DCC for use within mainland China.

DCC will process personal data from Secure Access China in a manner that is consistent with this Privacy Data Sheet. DCC is the personal information processor for the personal data processed to administer and manage the customer relationship and the personal information processor for the personal data processed by Secure Access China in order to provide its functionality.

1. Overview

Secure Access China is a cloud security service edge solution designed to allow users to securely connect to the Internet and private applications from any device located in mainland China.

Secure Access China may also integrate with third-party products, including Cisco features delivered through Cisco Security Cloud Control (provisioning and subscription management) and Cisco Secure Client (connectivity). The data collected by Cisco Secure Client is set forth in this Privacy Data Sheet. Please see the privacy data sheets for Security Cloud Control by visiting the Cisco Trust Portal, for information regarding the processing of personal data. DCC is not responsible for customer data once it leaves DCC’s control for a non-DCC product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

Please see Cisco Secure Access China for additional information.

2. Personal Data Processing

Table 1 lists the personal data processed by Secure Access China to provide its services and describes why the data is processed.

Table 1

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Account Data	• Dashboard/console users (each an “Admin”) first and last name • Admin email address • Company name, street, city, state/region, country, phone number • Admin IP address	• Activate, maintain, support, and improve the service • Billing, invoicing, and tax compliance • Export compliance • Notification of features and other updates • Authentication and authorization • Managing entitlements and renewals

Connection Data **(VPN-as-a-Service, Roaming)**	• Device private and/or public IP address • User ID and/or username • User Group IDs • Device IDs • Device name • Hardware UUID • Destination private application information (Application ID, IP, FQDNs) • Device Posture Data (below) • Personal data included in web traffic (HTTP/HTTPS), including headers, URLs, and cookies • Org ID • Active Directory (AD) or Identity Provider (IdP) GUID/ UPN if on-premise AD/cloud IdP is configured	• Provide, maintain, support, and improve the service • Enable secure connectivity to Internet and private applications
Device Posture Data	• Device public IP address • User ID • Device public key • Device identifiers (e.g., device ID, device/host name, machine GUID) • Device OS and version • Device configuration properties (e.g., is password set, is disk encryption enabled, is screen lock enabled) • WiFi fingerprint (snapshot of device location represented by hash value derived from visible SSID at time of capture)	• Provide, maintain, support, and improve the service • Assess and validate device's security and status in order to determine whether the device should be authorized to connect to the network or private application
Security Data	**Secure Web Gateway**[1]	
	• Personal data included in web traffic (e.g., headers, URLs, body content)[2] • Source and destination IP address • Origin ID • Org ID • Device ID • Timestamp • Proxy specific headers • Cloud apps associated with user or device • Personal data in inspected files	• Provide, maintain, support, and improve the service • Provide granular protection at URL and file level
	Firewall-as-a-Service	
	• Org ID • Private and/or public source and destination IP addresses • Application ID (public/private) • User ID • Packet content (for IPS feature)	• Provide, maintain, support, and improve the service • Provide granular protection at URL and file level
	Data Loss Prevention (DLP)[1]	

[1] Identity data (e.g., active directory, IdP, Google Workspace ID, username, userID and other identity information described under "Configuration Data") is not stored by DCC with Event Logs for this feature. The product pairs identity data with Event Logs at time of display in the dashboard, for purposes of reporting using Reporting API, and upon exporting Event Logs to a customer specific AWS S3 bucket if customers elect S3 export option.

[2] URL query parameters for HTTPS are not logged, however customers can opt-in to have full URL exported to an S3 bucket.

	Real-Time DLP • File name • File ID • Personal data in scanned SaaS environment, messages, files, and other content inspected by DLP • Snippet of text triggering violation and surrounding text • If configured, user identity data through AD/IdP • Real Time DLP will scan outbound and certain inbound traffic and any personal data included in such traffic. See Secure Access China User Guide for more information regarding Real Time DLP inbound and outbound scanning	• Provide, maintain, support, and improve the service • Discover, monitor, and act on (e.g., block) sensitive information (including personal data) in files, messages, and other customer content in transit through the Secure Access China service for Real-Time DLP
	Cloud App Discovery	
	Network traffic logs ingested by App Discovery based on the supported network data source(s), which may include: • User ID and/or e-mail address • User first and last name • Source IP address and associated cloud applications • Destination URLs	• Provide, maintain, support, and improve the service • Detect and provide risk score for cloud applications utilized by users
Control Plane Data (Configuration, Policies, Identity)	Configuration and Policy Data	
	• Audit logs which include Admin name • Policy settings which include Admin name and IP address • Object labels (e.g., roaming device and mobile device names) • Chromebook client email ID and/or device serial number and OS • Unique account ID (e.g., Org ID) • Any personal data in reports generated within dashboard (reports pull data from Event Logs stored in US and EU Event Log storage)	• Configuration Information is processed to log policies implemented and/or changed and the customer administrator who made the change • Provide information about the account • Provide reports requested by Admin
	User and Device Identity Data	
	• If using AD or IdP add-on: AD/IDP User and device identity (first name, last name, username, display name, email,	• Manage policies and pinpoint activity per user or device to deliver the service • Authenticate user and/or device

	GroupName, device ID, device name, UserID, Group ID)[3] - Source IP address - User Principal Name (UPN) - Device hostname - Device key (device ID format depends on device, for example for Chromebook it is a user's email or id or device's serial number) - Device serial number and OS - Google Workspace ID (if using Google Workspace integration)	
Support Data	- Name - Email - Phone number of the employee appointed to open the support ticket - Authentication information (exclusive of passwords) - Work organization and responsibilities - Customer provided case attachment data (including text, audio, video or image files). DCC does not intentionally collect or process personal data via customer case attachments. Customers should provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers.	- Provide remote access support - Review quality of the support service - Perform analysis of the service solution

Secure Access China collects “System Information” to assist DCC with understanding product usage, enabling product improvements and adoption. Any personal data that is processed as part of this Systems Information is protected in accordingly.

3. Data Center Locations

Secure Access China uses AWS data centers in China for the Secure Access China configuration, policies, reporting, and control plane (collectively, the “Control Plane”) and for data processing to provide security and enforce customer policies (collectively, the “Data Plane”). Please see tables and additional details below.

3.1 Data Processing

Table 2

Service	**Data Center Locations**
- Account Data - Control Plane Data (configuration, policies, identity) - Connection Data (VPN-as-a-Service, Roaming) - Device Posture Data	China

[3] URL query parameters for HTTPS are not logged, however customers can opt-in to have full URL exported to an S3 bucket.

If using user management services provided with the Secure Access China product to integrate with Google Workspace identities via Google’s APIs, DCC will processing data received from Google in accordance with the Google API Services User Data Policy, including the Limited Use requirements.

• Secure Web Gateway • Firewall-as-a-Service • Real-Time DLP • Cloud App Discovery • Support Data	

Cisco Security Cloud Control (SCC) and Cisco Secure Client are Cisco products (not DCC) that are included as part of the Secure Access China subscription. For SCC, customer personal data (e.g., admin username, email address) is processed and stored to the U.S. Please see the Security Cloud Control privacy data sheet by visiting the Cisco Trust Portal for more information. See Section 8 (Sub-processors) for other limited instances where data is sent outside of China. For Cisco Secure Client, customers must opt-out of the Customer Experience Module to prevent their data from being sent outside of China. See the Secure Access China documentation on opt-out instructions.

3.2 Data Storage

Data Plane usage and event data ("Event Logs") to the extent logging is enabled, and Control Plane data, are stored in the location referenced in Section 6. Customers have the option for most Event Logs to log nothing, log everything, or log only security data. Please see the Secure Access China product documentation for details on logging. Logging for intrusion prevention (IPS) is always on.

4. Cross-Border Data Transfer Mechanisms

When you use the Secure Access China service operated by DCC in the Chinese mainland region and/or use DCC technical support, all the personal data generated by you during the process of using the services will be stored within the territory of the People's Republic of China to the extent and as detailed in Sections 3 and 8, and such acts as storage and transmission all comply with the requirements of relevant laws and regulations of the People's Republic of China. It is specifically noted that, when related to DCC is resolving technical issues that occur during your use of the product/services or to the proper operation of the product, if it is necessary to transmit the customer's usage data and necessary personal information overseas, DCC will ensure that such transmission complies with the provisions of Chinese laws and regulations. If you do not wish for the personal information generated during your use of the Secure Access China products and services to be transmitted overseas, you will not be able to use this product.

5. Access Control

The table below lists the personal data used by Secure Access China to carry out the service, who can access that data, and why.

Table 3

Personal Data Category	Who has Access[4]	Purpose of the Access
Account Data	Authorized DCC and Cisco employees	Provision customer's account; billing/invoicing and tax compliance; export compliance; supporting the service subject to applicable data access and security controls
	Customer Admins	Enter, modify, control Admin data
Connection Data (VPN-as-a-Service, Roaming)	Authorized DCC and Cisco employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer Admins	View data on UI and through reporting. Data can be exported to S3 by opting into the data export option

[4] For Connection Data, Device Posture Data, Security Data and Control Plane Data, DCC does not access the data from a policy perspective, however, due to root access DCC has the ability to access this data.

Device Posture Data	Authorized DCC and Cisco employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
Security Data	Authorized DCC and Cisco employees	Deliver, support, maintain, improve the service
	Customer Admins	View data on UI and through reporting. Data can be exported to S3 by opting into the data export option
Control Plane Data (Configuration, Policies, Identity)	Authorized DCC and Cisco employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer Admins	Manage and configure account, establish, and maintain policies
Support Data	Authorized DCC and Cisco employees	Work with customer to resolve their support case
	Customer	Work with DCC to resolve their support case.

6. Data Retention

The table below lists the personal data used by Secure Access China, the length of time that data needs to be retained, why we retain it, and location of retention.

Table 4

Personal Data Category	Types of Personal Data Processed	Retention Period and Location[5]	Purposes for Retention
Account Data	See Table 1	Deleted upon request (China)	Retention of administrative data for legitimate business purposes
Connection Data (VPN-as-a-Service, Roaming)	Administrative service logs: • See Table 1 (excluding WiFi fingerprint from Device Posture Data)	Up to 90 days (China)	Troubleshooting service configuration and system errors
	Event Logs: • Device public/private IP address • User ID • Org ID • User Group IDs • Device IDs • Destination private application information • Device OS and version • Device configuration properties • Geolocation (derived from public IP address)	Up to 31 days (China)	Ongoing feature usage and reporting; troubleshooting
Device Posture Data	Application logs: See Table 1 (excluding WiFi fingerprint)	Up to 90 days (China)	Troubleshooting and debugging
	Routing logs: • Device public IP address • Org ID	Up to 365 days (China)	Troubleshooting and debugging

[5] In the unlikely event of a system crash, data in memory at the time of the crash (a "core dump") is automatically captured. A core dump is used to enable root cause analysis and remediation and may be retained in the U.S. to facilitate the engineering effort. Note, it may take up to 60 days to delete data pursuant to a data deletion request.

	Posture records: • See Table 1 (excluding IP address)	Deleted upon request (China)	Ongoing feature usage and reporting; troubleshooting
Security Data	Secure Web Gateway		
	Event Logs: • Source and destination IP • Origin ID • Org ID • Device ID • Timestamp • Proxy specific headers • URLs[2]	Up to 31 days (China)	Ongoing feature usage and reporting; troubleshooting
	Firewall-as-a-Service		
	Administrative Service Logs (generally no personal data, but data in Table 1 may be captured in error logs)	Up to 30 days (China)	• Troubleshooting and debugging
	Event Logs: • Org ID • Origin ID • Source and destination IP Application ID (public/private)	Up to 31 days (China)	• Ongoing feature usage and reporting; troubleshooting
	Data Loss Prevention (DLP)		
	Real-Time DLP Event Logs: • File name/File ID • Snippet of text and surrounding text (for context) triggering violation • If configured, user identity data through AD/IdP	12 months (China)	• Ongoing feature usage and reporting; troubleshooting • Inspected content is not retained except as noted
	Cloud App Discovery		
	• Cloud apps associated with user or device	90 days (China)	• Ongoing feature usage and reporting
Control Plane Data (Configuration, Policies, Identity)	Configuration and Policy Data		
	See Table 1	Deleted upon request[6] (China)	• Ongoing service usage and reporting; troubleshooting
	User and Device Identity Data		
	See Table 1	Deleted upon request (China)	• Ongoing feature usage and reporting; troubleshooting
Support Data	See Table 1	Deleted upon request (China)	• To ensure efficient support in case of recurring issues and to comply with DCC audit policies related to business records of services provided to Customers (i.e., legitimate business purposes)

For Cisco Security Cloud Control data retention and storage, see Section 3 above.

7. Personal Data Security

DCC has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Table 5

[6] Customer can revoke OAuth Keys at any time.

Personal Data Category	Type of Personal Data	Security Controls and Measures (Subject to notes below this Table)
Account Data	See Table 1	Encryption in transit and at rest
Connection Data (VPN-as-a-Service, Roaming)	See Table 1	Encryption in transit and at rest
Device Posture Data	See Table 1	Encryption in transit and at rest
Security Data	See Table 1	Encryption in transit and at rest
Control Plane Data (Configuration, Policies, Identity)	See Table 1	Encryption in transit and at rest
Support Data	See Table 1	Encrypted in transit and at rest

Encryption in transit means data is encrypted between Secure Access China data centers while traveling over the internet. Data is encrypted in transit from the user to the Secure Access China data center if the customer uses HTTPS or another encrypted communication method such as a secure tunnel. Some data may be unencrypted in transit between Secure Access services within the same data center. All data stored by Secure Access China (including back-ups) is encrypted at rest except as described in this paragraph.

Files and other traffic content are processed unencrypted, in memory, at the edge data center to complete the inspection and apply policies. Identity data is hashed while in the edge data center for processing using a randomly generated numeric ID. While a customer has the option for some Secure Access China packages to configure their traffic so that it will not be unencrypted at the edge data center, without this decryption, security can only be applied based on the IP address and domain metadata and a customer will not have the benefit of the full Secure Access China security.

Access to customer information is protected by multiple authentication and authorization mechanisms. There is an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based by roles and job functions.

8. Sub-processors

DCC partners with service providers that act as sub-processors of personal data. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Table 6

Sub-processor	Personal Data	Service Type	Location of Data Center
Atlassian (JIRA)	Support Data	To provide customer support	China
AWS China	See Table 1	Cloud infrastructure provider, Event Log data warehouse	China

Cisco	See Table 1 Account Data	Assist DCC in operation of the cloud service. Security Cloud Control (SCC)	China. Limited personal data (e.g., IP address) sent to the U.S. for assistance with service remediation, troubleshooting and support. Provide SCC service to customers. See Cisco Trust Portal for SCC Privacy Data Sheet
Grafana Labs	Administrative Service Logs	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	China
SendCloud	Email Header data Email body	Automated in-product emails such as password reset and account provisioning emails.	China

9. Exercising Data Subject Rights

Users whose personal data is processed by Secure Access China 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.

We will confirm identification 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 to DCC can be made by submitting a request via email to ciscohosting@dcclouds.com. We will endeavor to timely and satisfactorily respond to inquiries and requests.