



Offer Disclosure

Cisco Duo

This Offer Disclosure provides detailed information about data handling practices, security controls, and AI features specific to this Cisco Offer. It complements the [General Disclosure](#) which outline Cisco's overarching approach to handling Customer Systems Information and Customer Content, and the Cisco Online Privacy Statement, which offers a more in-depth explanation of how Cisco manages personal data. Together, these documents provide transparency by addressing data handling at both a high level and an Offer specific level, helping you understand how Cisco protects and processes information across its Offers.

Capitalized words not otherwise defined in this Offer Disclosure have the meanings set forth in the Cisco General Terms or General Disclosures. To the extent this document differs from the Cisco Online Privacy Statement or General Disclosures, this document will take precedence regarding Offer specific information. If there is a difference in the translated, non-English versions of this document, the US-English version will take precedence.

Cisco will review and update this disclosure on an annual basis, or as needed, to reflect material changes in the processing of Customer Systems Information or Customer Content. For updates, subscribe via the "subscribe" link in the upper right corner of the [Trust Portal](#).

1. Overview

Cisco Duo provides a SaaS-based solution for runtime identity and access management (IAM) controls, including Directory (IdP), multi-factor authentication (MFA), single sign-on (SSO), adaptive access authentication, and device trust & health checks. Its platform helps organizations verify user identities and device trust before granting access to applications, supporting both cloud and on-premises environments. Recently, Duo has fortified its offering with posture management ISPM and ITDR functionality, additional options for passwordless authentication/phishing-resistant MFA, and identity verification workflows. Duo enables organizations to enhance security and meet compliance requirements.

The following paragraphs describe Cisco's processing of Customer Content and Customer Systems Information in connection with the delivery of Duo, the location and transfers of that data, and how it is secured in accordance

with privacy principles, laws, and regulations. If you choose to use the Duo services, you will need to disclose personal data to Cisco. Cisco will use your personal data consistently with this Offer Disclosure.

Your use of Duo may include the option to use Cisco Identity Intelligence (CII). CII is an API-driven, cloud-native, and agentless platform that provides a unified view of all the identities within, and interacting with, an organization and then helps remediate risks at scale. Please see the Addendum for information on this capability and how it processes Customer Content and Customer Systems Information.

Additionally, Duo may integrate with third-party products, such as Persona to enable Duo Identity Verification. Cisco is not responsible for customer data once it leaves Cisco’s control for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

You may access the Cisco AI Assistant through Duo. The Cisco AI Assistant may include capabilities to assist customers in making informed decisions, augmenting tool capabilities, automating complex tasks, and searching Cisco documentation. Data related to your interactions with the Cisco AI Assistant is processed in accordance with the [Cisco AI Assistant Offer Disclosure](#).

Cisco AI Assistant services through Duo may direct your query entered in the AI Assistant outside your primary Duo deployment region for processing by the AI Assistant. Depending on your Duo deployment region, your AI Assistant query data may be routed to multiple locations within the same region (but not necessarily the same country) for processing and redundancy. Below are examples to illustrate how AI Assistant query data flows:

Primary Duo Deployment Region	Additional Cross-Region Routing for AI Assistant
US	United States
Canada	United States
EU	France, Ireland, Germany, Sweden
UK	France, Ireland, Germany, Sweden
DACH	France, Ireland, Germany, Sweden
Australia	Japan, Korea, Singapore, Australia, India
ASEAN	Japan, Korea, Singapore, Australia, India
Japan	Japan, Korea, Singapore, Australia, India
Middle East	Japan, Korea, Singapore, Australia, India
India	Japan, Korea, Singapore, Australia, India

Many Cisco Offers either require that the Offer be accessed through Cisco Security Cloud Control or optionally allow access to the Offer through Cisco Security Cloud Control. If you access this Cisco Offer through Cisco Security Cloud Control, please see the [Cisco Security Cloud Control Offer Disclosure](#) for further details regarding data handling and security controls.

For more information about Duo, visit <https://duo.com/docs>

2. Data Handling

2a. Collection, Purpose & Retention

Cisco believes in transparency when it comes to how Cisco handles Customer Content and Customer Systems Information. This disclosure provides details about the types of data Cisco collects, specific data elements involved, the purposes for which they are used, and how long Cisco retains them for this Cisco Offer.

Table 1: Customer Content

Data Category	Data Elements (Examples)	Purposes	Retention Period
End-User Registration and Authentication Information	Personal Data: • Username • Name • Date of birth¹ • Telephone number • Email address • A user's Active Directory username & password for those users authenticating via Duo hosted SSO (password is processed only long enough to complete each authentication and not retained after authentication) • A user's password if created for use with Duo Directory² • Custom Attributes defined and configured by Customer in Duo Directory (e.g., an employee's role, nickname, username, or office location)	• Account creation and activation • Service authentication and login • Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services	• 1 year (unless deleted sooner by customer) ³

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period
End-User Registration and Authentication Information	Non-Personal Data • Organization name • Group membership • User directory source(s) • User identifiers • Authentication configuration & status information (like locked out, bypass, e.g.)	• Account creation and activation • Service authentication and login • Deliver, support, improve security functionality, upgrade and improve the services	1 year (unless deleted sooner by customer) ³

¹ Duo provides customer administrators with the option to add a user's date of birth for the purposes of enabling Duo Identity Verification. Use of Duo Identity Verification requires integration with Persona. Customers must subscribe with Persona directly. For more information on Duo Identity Verification visit here: <https://help.withpersona.com/articles/1DfUf0PhctXPDY8s1sbOal/duo-verify-with-persona>.

² Duo adheres to industry best practices for password security by using strong hashing algorithms, high iteration counts, unique random salts for each password before hashing, and a secret per-customer pepper. Duo stores password hashes and salts in databases with strict access controls that are encrypted at rest.

³ Debug logs may reside in Duo's systems for up to 90 days after their creation for customer support purposes, security review, and to monitor and alert on patterns of system performance.

Account Registration Information	Personal Data of Administrator: - Name - Username - Telephone number - Email address - One-way hashed representations of password(s) for the Duo Administrator Panel - Job title - Billing and delivery address (if home address)	- Account creation and activation - Service authentication and login - Sending communications to you, including for marketing or customer satisfaction purposes, either directly from Cisco or from our partners - Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services	1 year (unless deleted sooner by customer)
Account Registration Information	Non-Personal Data: - Billing and delivery address (if corporate address) - Organization name - Role(s) - Group membership - Administrator directory source(s) - Administrator identifiers - Authentication configuration & status information (like locked out, bypass, e.g)	- Account creation and activation - Service authentication and login - Sending communications to you, including for marketing or customer satisfaction purposes, either directly from Cisco or from our partners - Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services	1 year (unless deleted sooner by customer)
End-User Device Metadata⁴	Personal Data: - Type of device - Device operating system, device version, and other device characteristics (e.g., if a device is “jailbroken” or has a screen lock in place) - IP address - Time zone - Time and date of authentication - Geolocation data - Broad geographic area (country or city-level location) - Application that device is attempting to access - The device’s fully qualified domain name associated with the end-user - Snapshot of device location represented by hash value derived from visible SSID at time of capture	- Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services Ensure secure devices and/or applications - Issue certificates verifying device is secure - Authenticate device - Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services - Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	1 year (unless deleted sooner by customer)
End-User Device Metadata⁴	Non-Personal Data included in End User Device Metadata, such as: - Connection information - such as encryption protocol(s) being used to access the Duo service - Browser type	- Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services Ensure secure devices and/or applications - Issue certificates verifying device is secure	1 year (unless deleted sooner by customer)

⁴ Duo Passwordless does not record or collect user biometric data in any way. Where available, it can request use of device biometric capabilities in a way that does not involve any biometric data leaving the device.

	- Whether a Public Key Infrastructure Certificate is installed - Whether device is utilizing certain plugins - Device identifiers (e.g., device name, processor ID, serial numbers, UDIDs, UUIDs, DNS Hostname)	- Authenticate device - Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services - Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	
Events Data ⁵	Personal Data: - Dates and times of access - IP address for determining where the services are accessed - Any personal data that may be included in device events (e.g., crashes, system activity, hardware settings)	- Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services - Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services - Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	1 year (unless deleted sooner by customer) ³
Events Data ⁵	Non-Personal Data included in Events Data, such as: - How end-users access the services - Any non-personal data that may be included in device events (e.g., crashes, system activity, hardware settings) - Success or failure of events - Transaction identifiers linking multiple events - Anonymous system identifiers of users and devices involved	- Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services - Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services - Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	1 year (unless deleted sooner by customer)
Authentication and Activity Logs	Personal Data: - Which end-users access the services - Time when the end-user accesses the service - End-user IP address when accessing the services	- Provide and maintain the services - Improve user experience - Improve security functionality - Improve quality of the services - Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services - Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	1 year (or less, depending on customer's log retention settings)
Authentication and Activity Logs	Non-Personal Data included in activity logs, such as: - Which devices access the services - Time when the devices access the service	- Deliver, support (including technical support), maintain, improve security functionality, upgrade and otherwise improve the services - Conduct statistical analysis with pseudonymized and/or	1 year (or less, depending on customer's log retention settings)

⁵ Events data refers to records or logs of specific occurrences, actions, or incidents that take place within a system, application, network, or environment. Events typically represent significant or noteworthy activities, such as user interactions, system events, errors, warnings, transactions, changes in state, or other noteworthy occurrences.

	• Applications protected by the services • Qualitative assessments of risk (detections) • Success or failure of actions taken • Transaction identifiers linking multiple logs • Anonymous system identifiers of users and devices involved	aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity	
Configuration Data⁶	Personal Data: • Configuration data is typically non-personal data but may include settings such as user preferences.	Configuration data is typically used to tailor the functionality of a system to specific requirements or preferences	1 year (unless deleted sooner by customer)
Configuration Data⁶	Non-Personal Data: • Configuration data may include non-personal data such as hardware settings, software configurations, network settings, and other customizable options. • Localization settings (language, timezone) • Account-wide security settings (password requirements, lockout settings, etc.) • Custom branding (customer logos, colors)	Configuration data is typically used to tailor the functionality of a system to specific requirements or preferences	1 year (unless deleted sooner by customer)
Business Analytics Data	Personal Data: • Admin first and last name • Job title • Admin Email address	• Internal business and product analytics and reporting to inform data-driven business and product decisions and product improvements • Product and feature usage analytics, sales support, renewal support, product adoption and deployment assistance • Email for product improvements or enhancements	Deleted upon request
Business Analytics Data	Non-Personal Data such as: • Company name • Admin role	See Purposes immediately above for Business Analytics Data	Deleted upon request

Regardless of the default retention referenced above, service backups are generated daily, encrypted, and moved into cold storage as a means of providing data integrity and resiliency for the services. Service backups are retained for an additional 3 years in such cold storage. This retention period was selected because it is sufficient to cover most scenarios wherein customers may request access to their historical data to serve their own legal discovery or forensics needs.

Pseudonymized Data: Duo additionally may retain copies of the data above, including the Personal Data Categories listed in the [Cisco AI Assistant Offer Disclosure](#) (if you use the Assistant through Duo), for the purpose of supporting

⁶ Configuration data refers to the settings or parameters that determine the behavior or operation of a system, application, device, or service.

the security, quality, and improved functionality of the service. In these copies, all personal data listed above is pseudonymized (except for IP addresses, which are needed in the original form for threat detection and related security reasons). In addition to the prompt data referenced in the Cisco AI Assistant Offer Disclosure, Duo may retain queries, responses, and associated metadata for the stated retention period. After the retention periods above have expired (or 1 year from collection in the case of IP Addresses), there will be no remaining production data or account information allowing for re-identification. To the extent any of the data above is also processed by the Cisco AI Assistant; it is retained in accordance with the [Cisco AI Assistant Offer Disclosure](#).

A user may request deletion of personal data at any time by contacting their Organization/Controller. Duo Account Administrators can reference the following article to process individual deletion requests: https://help.duo.com/s/article/2162?language=en_US.

Duo only keeps personal data for as long as it has an ongoing legitimate business need to do so. As such, we retain personal data associated with your account for as long as you have an active account using our services. This is necessary to provide core service functionality. Personal data will remain in the account until a validated account owner chooses to delete the data or requests an account closure. However, customers do have the ability to delete user/administrator registration information and logs, as set forth below (note that it may take up to 30 days for certain manually deleted data to fully purge from Duo's systems).

The Duo multi-tenant service is designed to provide strong guarantees around data integrity and availability of customer data. A core component of this architecture requires a balance between the need to purge data associated with previously deleted customers while ensuring that data associated with remaining active customers is properly maintained and protected.

2b. Storage and Processing

The Duo service is headquartered in the United States and operates internationally. Duo uses Amazon Web Services (AWS) data centers in the United States, Canada, Ireland, France, Germany, Switzerland, Australia, Japan, Singapore, Indonesia, the United Kingdom, India, and the UAE.

The Hosting region is automatically selected based on the country of the phone number during sign-up (or based on the country selected during certain methods of provisioning). The countries that are selected for each hosting region are listed in the table below. Customers may also request that their production hosting be in any region listed below. If you use the CII functionality of Duo, your personal data from this functionality will be hosted in accordance with the CII Addendum attached.

Duo maintains data within the customer's designated Hosting Region, though there are specific operational circumstances under which data may be processed or transmitted outside of that region. Support-related data may be transferred outside the hosting region to facilitate necessary debugging and maintenance activities. When a user accesses Duo while traveling outside their hosting region, their data is encrypted and routed through the closest physical network endpoint to the hosting region, unless the customer has specifically configured Duo to

restrict access to within the hosting region. Additionally, for purposes of service continuity and resilience, data may be transferred outside the hosting region as part of the [Duo Business Continuity and Disaster Recovery Plan](#). In addition, if a customer selects voice or text for multi-factor authentication (MFA), then the user’s phone number may leave its hosting region and get transmitted to the US to Duo’s telephony provider. Some limited data may also leave the hosting region when processed by Duo’s non-telephony service providers, which act as sub-processors (see Table 4 below).

Table 3: Data Centers

Region	Infrastructure Provider	Automatically selected during sign-up for phone numbers from these countries	Data Center Locations
United States	AWS	California Oregon	Multiple regions and availability zones in the United States.
Canada	AWS	Canada	Multiple regions and availability zones in Canada.
EU	AWS	Belgium, Bulgaria, Croatia, Cyprus, Czech Republic (Czechia), Estonia, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain Additionally, any other country in the world, not listed in this table, will default to the EU data center.	Single regions and multiple availability zones in France and Ireland.
DACH	AWS	Germany, Austria, Switzerland, Denmark, Finland, Iceland, Norway, and Sweden	Single regions and multiple availability zones in Germany and Switzerland.
ANZ	AWS	Australia, Cook Islands, Fiji, French Polynesia, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, New Caledonia, New Zealand, Niue, Pitcairn, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis and Futana	Multiple regions and availability zones in Australia.
Japan	AWS	Japan	Multiple regions and availability zones in Japan.
ASEAN	AWS	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam	Single regions and multiple availability zones in Singapore and Indonesia.
United Kingdom	AWS	United Kingdom, British Overseas Territories	A single region and multiple availability zones in the United Kingdom.
India	AWS	India	Multiple regions and availability zones in India.
UAE	AWS	Bahrain, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, UAE	A single region and multiple availability zones in the UAE

Service Providers. Cisco may share Customer Systems Information and Customer Content with a trusted ecosystem of suppliers. In each instance, each participant has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco’s commitments to you.

Subcontractors assist with broader data processing services, while subprocessors specifically process Personal Data on Cisco’s behalf to support the functionality of the Cisco Offer. Both are listed below. For updates, subscribe via the “subscribe” link in the upper right corner of the Trust Portal.

Table 4: Subprocessors and Subcontractors

Name	Personal Data	Service Type	Cisco Data Center Location
AWS	End-User Registration/Authentication Information, End-User Device Metadata, Account Registration Information, Events Data, Authentication & Activity Logs	Cloud based infrastructure and hosting, analytics, data storage	US (California, Oregon), Canada, Ireland, Germany, Australia, Japan, Singapore, the United Kingdom, India, and the UAE
Twilio, Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US (Oregon, Virginia)
Nexmo Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US (California, Oregon, Virginia)
Clickatell, Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US (California, Oregon, Virginia)
Bandwidth Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US (California, Oregon, Virginia)
Google	End-User Registration/Authentication Information	Push notifications for authentication	US (California, Nevada, Ohio, Virginia), Ireland
Salesforce	Account Registration Information	Deliver, support, and improve the services	US (Arizona, Texas)
Mulesoft	Account Registration Information	Assist with Salesforce integration	US (California, Oregon, Virginia)
Marketo	Account Registration Information	Automated account management	US (California, Virginia)
Amplitude	Events Data	Analyze feature usage and product functionality	US (Virginia, Ohio, Oregon, California)
Sentry	Events Data	Error Reporting	US (Iowa)
Snowflake	End-User Registration/Authentication Information, End-User Device Metadata, Account Registration Information, Events Data, Authentication & Activity Logs, Business Analytics Data	Analytics and data storage	US (Virginia)

2c. Access and Sharing

Customers and their authorized third parties may directly access Data by using standard APIs, to the extent those are described in the API documentation found [here](#).

Duo APIs may support both structured and unstructured data sets depending on the particular data set requested from Duo. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other

standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

Customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels.

3. Security

3a. Access Control and Encryption

Cisco has implemented reasonable and appropriate technical and organizational measures designed to protect data from accidental loss, unavailability, and unauthorized access, use, alteration, and disclosure.

Table 5: Access & Controls

Data Category	Who Has Access	Purpose of Access	Security Controls
End-User Registration / Authentication Information	Customer administrator	Modify and control access to the services and other administrator information	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Support the services in accordance with its data access and security controls process	
Account Registration Information	Customer administrator	Modify and control access to the services and other administrator information	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Deliver, support, upgrade and improve the services	
End-User Device Metadata	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Deliver, support, upgrade and improve the services	
Events Data	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Deliver, support, upgrade and improve the services	
Authentication and Activity Logs	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Deliver, support, upgrade and improve the services	

Configuration Data	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
	Cisco	Deliver, support, upgrade and improve the services	
Business Analytics Data	Cisco	Organize, analyze, and report on business and product usage data; improve the service	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.

3b. Reports & Resources

In addition to complying with internal standards, Cisco maintains third-party validations and certifications to demonstrate its commitment to robust information security and privacy. The General Disclosures describe Cisco's enterprise-wide certifications. The following additional resources and certifications apply specifically to this Offer:

- [Trust Package](#)
- [ISO Documents](#)
- [SOC Documents](#)
- [C5 Documents](#)
- [CAIQ](#)
- [ENS Certification](#)
- [HIPAA Assessment](#)
- [CSA STAR Certification](#)

Cisco Identity Intelligence Addendum

This Offer Disclosure Addendum for Cisco Identity Intelligence (CII) outlines Cisco’s overarching approach to handling Customer Systems Information and Customer Content, and the Cisco Online Privacy Statement, which offers a more in-depth explanation of how Cisco manages personal data. Together, these documents provide transparency by addressing data handling at both a high level and an Offer specific level, helping you understand how Cisco protects and processes information across its Offers.

1. Overview of Cisco Identity Intelligence

Cisco Identity Intelligence (CII) is an API-driven, cloud-native, and agentless platform that provides a unified view of all the identities within, and interacting with, an organization and then helps remediate risks at scale.

This Addendum only addresses the CII feature. For information regarding the processing of personal data by Duo, please see the Duo Offer Disclosure to which Addendum 1 is attached. CII is inclusive of data categories as displayed in Table 1 and 2 above in the Duo Offer Disclosure. In addition to CII’s integrations with other documented Cisco Offers, this Cisco Offer can integrate with Cisco Cloud Control and Cisco AI Canvas, part of Cisco’s AI-native unified management experience. As part of this integration, the data from this Cisco Offer is transferred and processed as outlined in the [Cisco Cloud Control Offer Disclosure](#) and the [Cisco AI Canvas Offer Disclosure](#).

If You elect to use the OpenAI integration with Your CII license, the data attributes from that service will be sent to CII. The data attributes may be found here: <https://help.openai.com/en/articles/9261474-openai-compliance-platform-for-enterprise-customers>.

2. Data Handling

2a. Collection, Purpose & Retention

Cisco believes in transparency when it comes to how Cisco handles Customer Content and Customer Systems Information. This disclosure provides details about the types of data Cisco collects, specific data elements involved, the purposes for which they are used, and how long Cisco retains them for this Cisco Offer.

Table 1: Customer Content

Data Category	Data Elements (Examples)	Purposes	Retention Period
Admin Personal Data	Personal Data: • Username • Name • City • Country	• Account creation and activation • Service authentication and login • Sending communications to you, including for marketing or customer satisfaction purposes,	Deleted upon customer request

		either directly from Cisco or from our partners Deliver, support, improve security functionality, upgrade and improve the service	
Subject Data	Personal Data: - Name - Username - Telephone number - Email address - Login History (including city and county) Employment information (including directory role, directory organization, directory reporting structure, directory title, directory department, directory location)	- Account creation and activation - Service authentication and login - Deliver, support, improve security functionality, upgrade and improve the services	Deleted upon customer request

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period
Admin Audit Log	Personal Data: - Name - User Email - Login History	Service availability and support	1 year (unless deleted sooner by customer)
Admin Audit Log	Non-Personal Data: Action History	Service availability and support	1 year (unless deleted sooner by customer)

2b. Storage and Processing

CII uses Amazon Web Services (AWS) data centers in the United States, Canada, UK, Germany, Australia, Singapore, India, and Japan.

Hosting region is selected based on the country of the customer's Duo deployment is located or where parties mutually agree, except where customer is using CII through their XDR or Secure Access entitlements. In those cases, the CII hosting region will default to the regions customer selected for XDR and Secure Access. The countries that are selected for each hosting region are listed in the table below.

Table 3: Data Centers

Region	Infrastructure Provider	Countries Supported	Data Center Locations
United States	AWS	United States and all other countries not listed below	US (Ohio)
Canada	AWS	Canada	CA (Montreal)
Europe	AWS	European Economic Area (EEA)	EU (Frankfurt)

UK	AWS	UK	EU (London)
ANZ	AWS	Australia	AP (Sydney)
Japan	AWS	Japan	AP (Tokyo)
India	AWS	India	AP (Mumbai)
Singapore	AWS	Singapore	AP (Singapore)

Service Providers. Cisco may share Customer Systems Information and Customer Content with a trusted ecosystem of suppliers. In each instance, each participant has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco’s commitments to you.

Subcontractors assist with broader data processing services, while subprocessors specifically process Personal Data on Cisco’s behalf to support the functionality of the Cisco Offer. Both are listed below. For updates, subscribe via the “subscribe” link in the upper right corner of the Trust Portal.

Table 4: Subprocessors and Subcontractors

Sub-processor	Data Processed	Service Type	Location of Data Center
AWS	Subject Data and Admin Personal Data	Cloud based infrastructure and hosting, analytics, data storage	US (Ohio), Germany, UK, Australia, and Japan
Snowflake	Subject Data and Admin Personal Data	Data Storage and analytics	Co-located with AWS account US (Virginia)
Datadog	Subject Data and Admin Personal Data	Data Storage and analytics	US (Virginia)

2c. Access and Sharing

Customers and their authorized third parties may directly access Data by using standard APIs, to the extent those API’s are described in the API documentation found [here](#).

APIs may support both structured and unstructured data sets depending on the particular data set requested. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

Customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels.

3. Security

3a. Access Control and Encryption

Cisco has implemented reasonable and appropriate technical and organizational measures designed to protect data from accidental loss, unavailability, and unauthorized access, use, alteration, and disclosure.

Table 5: Access & Controls

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

Data Category	Who Has Access	Purpose of Access	Security Controls
Admin Personal Data	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)
	Cisco	Support the services in accordance with its data access and security controls process	
Admin Audit Log	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)
	Cisco	Support the services in accordance with its data access and security controls process	
Subject Data	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)
	Cisco	Support the services in accordance with its data access and security controls process	

3b. Reports & Resources

- Refer to 3b above in the Duo Offer Disclosure