



Offer Disclosure

Webex Contact Center Enterprise

This Offer Disclosure provides detailed information about data handling practices, security controls, and AI features specific to this Cisco Offer. It complements the [General Disclosures](#), 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 Webex Contact Center Enterprise ("Webex CCE" or the "Service") delivers intelligent contact routing, by combining multichannel automatic call distribution functionality with telephony in a unified solution. The Service is made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users ("Users" or "Agents") and people who access contact centers enabled by the Service (each an "End-User"). A Customer may purchase the Service through a Cisco partner ("Partner").

The Webex CCE solution is accomplished by call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. Webex CCE is powered by Cisco's Collaboration Solution for Contact Center and Unified Communications (UC). The major services provided are Contact Center as a Service (CCaaS) and Unified Communications as a Service (UCaaS) for contact center agents. Cisco Unified Communications Manager (CUCM) is the core call processing software for the Cisco Unified Communications System.

Because the Service enables collaboration among its users through voice conversations and text, personal data may be stored with the use of the Service. The following describes Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. If you choose to purchase the Service, you will need to disclose personal data to Cisco in order to use it. Cisco will use personal data consistent with this Offer Disclosure.

The Service may integrate with various Cisco products, including Webex Calling Dedicated Instance, Webex Connect, and Webex Contact Center, Webex Connect, Webex WFO, and Webex Control Hub. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving and sending personal data from and to the Service.

Note, the Service may also be integrated with products that the customer purchased from third parties (including purchases through Cisco's Solutions Plus resale program). Cisco is not responsible for customer data once it leaves the Service 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.

For more information about Webex Contact Center Enterprise, visit

<https://www.cisco.com/c/en/us/products/contact-center/webex-contact-center-enterprise/index.html>.

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
Customer Content	Personal Data: - Call Recordings (Optional with Webex WFO) - Transcriptions of calls (Optional with AI Agent or AI Assistant)) - Chat transcripts - Screen Captures (Optional with Webex WFO) - Emails	- Provide the Service - Ensure quality and training - Diagnose technical issues - Improve the Service	When you are an active customer: Cisco will retain this information as long as Customer has an active subscription Upon termination/expiration: After Customer has terminated the Service, Customer Content will be deleted within 28 days
Webex-Generated Content	Personal Data: AI Generated Content (optional, only applicable if AI Agent, AI Assistant, Webex WFO features are enabled by you).	Provide the Service	When you are an active customer: AI-Generated content with AI Agent, AI Assistant, Webex WFO per customer's contractual requirements Upon termination/expiration: Deleted within 60 days

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period
Administrative Data (Admins)	Personal Data: - Name - Username - Email Address - Password - IP Address - Active Directory Information (optional) - Phone Number	- Provide the Service - Enroll you in Webex CCE - Improve the Service - Authenticate / authorize access to Webex CCE - Provide support - Understand how the Service is used - Route calls - Display information to other Agents - Send product notifications	When you are an active customer: Cisco will retain this information as long as Customer has an active subscription Upon termination/expiration: After Customer has terminated the Service, Agent or User Information will be deleted within 28 days
Administrative Data (Users)	Personal Data - Name - Email Address - Phone Number - User ID or display name - Other/Customized data (this is defined and configured by Customer – it may contain personal data) - IP address	- Provide the Service - Improve the Service - Provide support - Understand how the Service is used - Route calls - Display information to other Agents	When you are an active customer: Cisco will retain this information as long as Customer has an active subscription Upon termination/expiration: After Customer has terminated the Service, End- User Information will be deleted within 28 days

	Data provided by end-user through Dual Tone Multiple Frequencies (DTMF)		
Configuration Data	Personal Data: - User Settings Non-Personal Data: - Settings - Hardware Settings - Software Configuration - Network Settings	Configure Functionality	When you are an active customer: Cisco will retain Configuration Data as long as Customer has an active subscription Upon termination/expiration: After Customer has terminated the Offer, Agent or User Information will be deleted within 28 days
Events Data	Non-Personal Data: Logs	- Troubleshooting - Auditing - Monitoring - Analysis - Reporting	When you are an active customer: After Customer has terminated the Offer, Events Data will be deleted within 60 days Upon termination/expiration: Other Events Data may be retained and deleted after 1 year
Telemetry Data	Personal Data: Agent Identifier Non-Personal Data: - Client Version - Device Information (e.g., phone type) - MAC Address - Software Version - Message Logs - Call Information, including durations, hold time, called number, calling number, time, date	- Understand how the Service is used - Provide support - Diagnose technical issues - Provide the Service - Improve the Service	When you are an active customer: Cisco will retain this information as long as Customer has an active subscription Upon termination/expiration: After Customer has terminated the Service, Calling Information will be deleted within 60 days. Telemetry may be retained and deleted after 1 year

2b. Storage and Processing

Data Centers. Cisco uses its own data centers as well as third-party infrastructure providers to deliver this Cisco Offer’s capabilities globally.

Table 3: Data Centers

Cisco Data Center Locations
Australia
Brazil

Tokyo
Netherlands
Singapore
United Kingdom
United States (Colorado, Texas)

Note: When you purchase a subscription, Cisco creates, processes, and stores your information in the United States regardless of the subsequent provisioning of your accounts in a chosen regional cloud. All data is encrypted in transit.

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.

Sub-contractors assist with broader data processing services, while sub-processors 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 5: Sub-processors

Name	Personal Data	Service Type	Cisco Data Center Location
Google (Optional)	Customer Content	Google CCAI provides transcription services. This service is provided in the region where Customer is provisioned. When a Google CCAI customer creates a project in the GCP portal, that customer may select where certain Customer Data will be stored, and Google will store it there in accordance with the Service Specific Terms found here.	Google Cloud Platform data storage facilities are located here. in these countries and regions https://cloud.google.com/about/locations
Calabrio (Optional)	Voice Communication Recordings; Screen Recordings; and Webex WFO-related content	Quality Management, Work Force Management,	Calabrio Data Center locations include the following: USA: Ohio, Oregon and Virginia Canada: Montreal, Quebec

		Analytics, and Cloud Infrastructure Storage	LATAM: Sao Paulo, Brazil EU: Dublin, Ireland UK: London, England ANZ: Sydney, Australia SGP: Singapore
Amazon Web Services	Administrative Data	To facilitate email transfers (Simple Email Service)	USA: Oregon
Microsoft Azure Cloud (Optional)	Agent and User Generated Data; and Webex-Generated Content.	Microsoft Azure is used to provide the optional AI Agent and AI Assistant services.	Data Center locations include Australia, Canada, the EU, India, Japan, Singapore, South Africa, Switzerland, UAE, UK, and US.

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](#) and [here](#), subject to the provisions of [Webex for Developers Terms of Service](#).

Webex Contact Center Enterprise APIs 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.

Cisco makes certain Customer Systems Information available to Customers and their authorized third parties in a structured, commonly used machine-readable format through the following standardized APIs, consistent with the specifications provided in the Cisco API Guidelines.

- Configuration <https://developer.webex.com>

Customers may send requests for expanded API or data interface capabilities through their 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 6: Access & Controls

Data Category	Who Has Access	Purpose of Access	Security Controls
Admin Registration Data	Cisco Customer	- Configure system for use by the Customer - Support the Service in accordance with Cisco's data access and security controls process - Access, manage, edit and view users	- Encrypted in transit and at rest - Passwords encrypted and hashed in transit and at rest
User Registration Data	Cisco Customer	- Support the Service in accordance with Cisco's data access and security controls process - Access, manage, and view use of the Service	- Encrypted in transit and at rest - Encrypted in transit and at rest
Telemetry Data	Cisco Customer	- Support and improvement of the Service. - Access and view Service usage and configuration information	Encrypted in transit and at rest
Customer Content	Cisco Customer	- While Cisco operates the Service, Cisco will not access the data unless it is shared with Cisco by the Customer and will only access in accordance with Cisco's data access and security controls - Access, view, modify, control, and delete in accordance with Customer's personal data policy	- All User-Generated Information is encrypted in transit and at rest - Data may not be encrypted for Real Transfer Protocol Traffic transmitted on private or local protected networks

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:

- [Webex Contact Center Enterprise Trust Package](#)
 - o ISO 27001/17
 - o ISO 27017:2015
 - o ISO 27018:2019
 - o SOC2
 - o PCI-DSS
 - o HIPAA
 - o PCI- DSS
 - o SOC 2 Type II Attestation

- o HIPAA Attestation
- o ISO 27017:2015
- o ISO 2700/17

4. Artificial Intelligence

Cisco prioritizes trust and transparency, including when it comes to development and deployment of AI. This disclosure provides an overview of the generative and agentic AI features included in this Cisco Offer:

Table 7: Generative and Agentic AI

Feature	Technical Note
Contact Center: Agent Answers and Suggested Responses	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=AI%20Transparency&prodserv=Cisco%20Webex%20Contact%20Center%20Service#/19784895250237237
Contact Center: Call Summaries and Handoff to Agent	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=AI%20Transparency&prodserv=Cisco%20Webex%20Contact%20Center%20Service#/19496680491489903
Contact Center: Topic Analysis	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=AI%20Transparency&prodserv=Cisco%20Webex%20Contact%20Center%20Service#/19529591075591898
Contact Center: Webex Workforce Optimization Enhancements	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=AI%20Transparency&prodserv=Cisco%20Webex%20Contact%20Center%20Service#/19128350572093407
Webex AI Agent	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=AI%20Transparency&prodserv=Cisco%20Webex%20Contact%20Center%20Service#/19445370048945010