



Offer Disclosure

Webex Connect

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 Connect enables rapid automation of customer interactions across various communication channels. The platform simplifies interactions between business enterprises and their customers around the world, across multiple channels like SMS, MMS, Voice, Email, Push Notifications, In-App Messaging, Live Chat, RCS, WhatsApp, Apple Messages for Business, Facebook Messenger, and other messaging apps. Cisco Webex Connect integration capabilities and visual flow builder allow users to build and launch workflows to support bi-directional customer interactions that work across supported channels and systems. With its low-code toolset and high-performance runtime engine, Cisco Webex Connect enables developers, product managers and architects to accelerate their CX transformation projects.

Cisco Webex Connect includes the following optional features:

- Cisco Webex Connect Contact Policy: a consent management tool which provides capabilities for maintaining records of customer consent preferences for various communications purposes, and for managing contact frequency.

- Webex Bot Builder: a tool to support the automation of tasks through AI. Available tasks include Text Summarization, Generating Code with a Natural Language Input, and Training Data Generation.
- Hospital Appointment SMS Reminder service: for UK NHS (National Health Service) Customer

Cisco Webex Connect supports integration with various Cisco products. Please see the applicable Disclosure Document on the Trust Portal for details regarding processing of personal data by the Cisco product receiving personal data from Webex Connect.

- Cisco Webex NMX Gateway
- Cisco Webex Smarthub Gateway

Note, Cisco Webex Connect may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves Cisco Webex Connect or 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 Cisco Webex Connect, visit <https://cpaas.webex.com/products/webex-connect>.

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

Customer Content			
Data Category	Data Elements (Examples)	Purposes	Retention Period
Host and Usage Information	Personal Data: • IP address • JSON web tokens • KPI logs • LDAP (Lightweight Directory Access Protocol) customer information • Mobile device identity • Tenant ID • Tenant name	• Provision and delivery of the service to Customer end users • Maintain user session connectivity to the service • Diagnose technical issues • Provide endpoint security • Provide security analytics and forensics	6 months Variations: • Live chat / in-app messaging: custom retention period can be configured, up to a maximum of 6 months.

	- Customer first name and last name - Customer email address - Customer mobile phone number - Customer business phone number - Customer user log-in credentials - Customer Accounts Payable - Customer UserID / e-mail address - Customer end user data for the following channels: SMS, MMS, Voice, and RCS : - mobile phone number - Geolocation (RCS) WhatsApp - User Name - WhatsApp Phone Number - WhatsApp Identity Hash - geolocation Facebook Messenger: - PSID (Facebook ID) - Name - Gender - Profile Picture Email Channel - Email ID - IP address Live Chat / In-App Messaging - User ID - Device ID - Push ID Push Notifications - Push ID Apple Messages for Business - User ID i.e., Opaque ID Contact Policy Module - mobile phone number - email address	- Provide malware analysis and threat intelligence - Respond to customer support requests - Customer accounts Payable for account reconciliation and billing	- Email channel: custom retention can be configured for Email IDs within a Bounce List, up to a maximum of 365 days. - Contact Policy Module: for the lifetime of the Customer's Active Account. - Mailgun: three days - For NHS Customers: two years in live and two years in archive
Registration Data	Personal Data: - Customer Name - Customer email address - Phone number (optional) - Customer ID - User level account details	- Provision and enroll you in the service - Authenticate and authorize access to the service - Enable product operations and functionality - Communicate on status and availability of service - Send product and support notifications	6 months

User Generated Data	Personal Data: • Messages (for SMS, MMS, RCS, WhatsApp, Facebook Messenger, Live Chat / In-App Messaging, Push Notifications, Apple Messages for Business) • Email messages and attachments • Content uploaded or shared • Uploaded media files • Voice messages Webex Bot Builder • Content uploaded or shared • Uploaded Media Files For healthcare providers (children and 18+) some or all of the following • Address • Age • Date of birth • Email • Home phone number • Mobile phone number • Medical information • Name • Language known • NHS number • Hospital Number • Messages • Email messages and attachments • Content uploaded or shared	• Enable product operations and functionality • Provide data processing services for voice recording and transcriptions (optional) Webex Bot Builder • Data Processing (processor), Perform contractual requirements (processor), Successfully run its operations (processor)	6 months Webex Bot Builder • User and bot message data - 90 days default retention (can be set to anything between 30-180 days based on customer requirements). • Analytics data containing number of sessions, messages, etc. - 730 days. • For NHS Customers: Two years in live, plus two years in archive
System Generated Data	Personal Data: • Audit records • Call data records • Call details • Call metadata • Email body • Email data header • Email sender (from email address) • End-user IP address [children healthcare providers] • End-user phone number • Log files [children and 18+ healthcare providers] • User agent	• Enable product operations and functionality	6 months • For NHS Customers: Two years in live, plus two years in archive
Support Information	Personal Data: • Customer ID • Customer Information • Support Case Details • Support Case Notes • Support Contact Information	• Diagnose technical issues • Ensure product operations and functionality are available to customers • Send product and support notification	• 6 months

Table 2: Customer Systems Information

Customer Systems Information			
Data Category	Data Elements (Examples)	Purposes	Retention Period
Configuration Data	Personal Data: User Settings	Configure functionality	For as long as the Customer is using the Offer
	Non-Personal Data: - Settings - Hardware Settings - Software Configuration - Network Settings		
Events Data	Non-Personal Data: Logs	- Troubleshooting - Auditing - Monitoring - Analysis - Reporting	6 months
Telemetry Data	Non-Personal Data: - Measurements - Readings - Status updates - Performance metrics - Environmental conditions	- Monitoring - Analysis - Reporting	6 months

2b. Storage and Processing

Data Centers

For this Cisco Offer, Cisco leverages third-party infrastructure providers to deliver this Cisco Offer’s capabilities globally.

Table 3: Data Centers

Infrastructure Provider	Infrastructure Provider Locations
Amazon Web Services (AWS) North America Cloud	Oregon, USA
Amazon Web Services (AWS) North America Cloud	Montreal, Canada
Amazon Web Services (AWS) UK Cloud	London, United Kingdom
Amazon Web Services (AWS) EU Cloud	Dublin, Ireland
Amazon Web Services (AWS) Asia Pacific Cloud	Singapore
Amazon Web Services (AWS) Asia Pacific Cloud	Sydney, Australia
Amazon Web Services (AWS) Asia Cloud	Mumbai, India
Microsoft Azure North America Cloud	North America (USA)

Note: When you use this Cisco Offer, your information is usually stored and processed in the data center closest to your principal place of business as provided to Cisco during the ordering process. For example, purposes only, if you are based in Europe your information will usually be stored and processed in the AWS EU Cloud.

*For UK NHS Customers, patient information will be stored and processed in the United Kingdom.

All data is encrypted in transit.

For this Cisco Offer, the infrastructure for this Cisco Offer runs on Amazon Web Services (AWS) or Azure in a single region in the location closest to your principal place of business and as provided in the table above – and spans multiple availability zones (AZs)

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: Subcontractors

Subcontractors		
Name	Service Type	Data Center Location
AWS	AWS cloud infrastructure is used to host Cisco Webex Connect. Data is retained for the durations specified in section 2.	Australia Canada India Ireland Singapore United Kingdom Oregon, United States Virginia, United States
Amplitude	Analyses Customer user actions to better understand how the service is being used and can be improved.	United States
Mailgun	If you choose to use the service to send emails, we use this service provider to deliver the emails.	United States
Microsoft Azure	Azure cloud infrastructure is used to host Cisco Webex Connect. Data is retained for the durations specified in section 7.	Virginia, United States

Table 5: Subprocessors

Subprocessors

Name	Personal Data	Service Type	Data Center Location
Amazon Web Services (AWS)	• Host and Usage Information • Registration Data • System Generated data • User Generated Data	AWS cloud infrastructure is used to host Cisco Webex Connect. Data is retained for the durations specified in section 2.	USA Australia Canada India Ireland Singapore UK
Microsoft Azure	• Host and Usage Information • Registration Data • System Generated Data • User Generated Data	Azure cloud infrastructure is used to host Cisco Webex Connect. Data is retained for the durations specified in section 2.	USA
Mailgun	• Host and Usage Information	If you choose to use the service to send emails, we use this service provider to deliver the emails.	USA
Amplitude	• Customer Email Address	Analyses Customer user actions to better understand how the service is being used and can be improved.	Local deployment based on Customer location
Sendgrid (Twilio)	• Customer Email Address	Description from PIA: Used this as SMTP server for sending out emails being generated at application level Eg offline reports scheduled at application chat transcript requests via email, email reset requests.	USA
Meta Platforms	• Host and Usage Information	Sending of WhatsApp messages, Facebook Messenger messages	USA
Apple Inc	• Host and Usage Information	Sending of Apple Messages for Business	USA

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

Webex Connect APIs support both structured and unstructured data sets depending on the particular data set requested from Webex Connect. 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](#).

[API Documentation](#):

- [Configuration](#)
- [Telemetry](#)
- [Events](#)

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

To the extent that any information comprising Cisco's algorithms, analysis, inferences, proprietary software, insights, derivations, or assigned values can be viewed, reverse engineered, reconstituted, or otherwise interpreted from the data, such information is a "Cisco Trade Secret," and subject to such confidentiality obligations.

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
Host and Usage Information	Cisco	• Enable product operations and functionality • Deliver, support, and improve the service in accordance with Cisco data access and security controls process • Account reconciliation and billing	• Encrypted in transit and at rest
Registration Data	Customers	• Configure, manage and operate the service • Modify, control and delete information • Manage users and administer service in accordance with your policies • Access, modify, and delete content in accordance with your personal data policy • Use the portal	• Encrypted in transit. Passwords are hashed and role-based access measures are applied at rest.
	Cisco	• Enable product operations and functionality • Deliver, support, and improve the service in accordance with Cisco data access and security controls process • Create accounts • Grant access to the portal	

User Generated Data	Customers	• Access, modify, and delete content in accordance with your personal data policy • Obtain reported information	• Encrypted in transit and at rest
	Cisco	• Deliver, support, and improve the service in accordance with Cisco data access and security controls process	
System Generated Data	Customer	• Manage users and administer service in accordance with your policies • Modify, control, and delete features • Upload files for security analytics and forensics • Set policies, view incidents, troubleshoot	• Encrypted in transit and at rest
Support Information	Cisco	• Deliver, support, and improve the service in accordance with Cisco data access and security controls process	• Encrypted in transit and at rest

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. For this Cisco Offer any additional resources and certifications are available at the [Cisco Trust Portal](#), including following:

- [Trust Package for Webex Connect](#)
- [CAIQ](#)

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
Code Generation AI Transparency Technical Note	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=webex%20connect#/19655099133946162
Text Summarization AI Transparency Note	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=webex%20connect#/19205125276337042
Training Data Augmentation AI Transparency Note	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=webex%20connect#/19248354195562999