EUROJUST
The European Union's Judicial Cooperation Unit
P.O. Box 16183 – 2500 BD The Hague • The Netherlands

DATA PROTECTION NOTICE
For processing of personal data in the context of the use of WebEx meetings

1. Context and Controller

As Eurojust collects and further processes personal data, it is subject to *Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*.
Collection and processing of personal data within Eurojust system log files is under the responsibility of the Controller, who is the Head of Information Management Unit and can be contacted at IMSecretariat@eurojust.europa.eu.

2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?

Legal basis

The legal basis for processing of personal data are:

Regulation (EU) 2018/1725 of 23 October 2018 (a2) (a) as per recital 22, second sentence

To be able to maintain and support IT systems needed for the operation of Eurojust.

Purpose of the processing

The WebEx Meetings solution is used for organising large-scale meetings hosted by Eurojust for internal and external participants, where non-operational, non-confidential, nor sensitive data (operational or administrative) are discussed or disclosed.

Technical means

Cisco uses two Data Centres in Europe at the moment to provide their services: Amsterdam and London. Cisco has in place a migration plan to move the services from London to the new Data Centre in Frankfurt post Brexit 2020, as explained in the attached FAQ on transfer of data.

Additionally, in the Eurojust configuration model set up with Cisco, the data are not shared with third countries, with the exception of the billing data which are sent and stored in the US Data Centre.

The data sent to the Cloud are encrypted as described in the attached Privacy Data Sheet, Meeting Security, and WebEx Control Hub.

Types of personal data

Personal data collected and further processed are:

1) **For Eurojust Staff Members managing the back-end/configuration portal (Back Office, Front Office)**

- Name
- Email Address
- Password
- Public IP Address
- Browser
- Phone Number (Optional)
- Mailing Address (Optional)
- Geographic region – obtained from the IP address

• Avatar (Optional)
• Billing Information
• Unique User ID (UUID) – as generated by Cisco and encrypted.

2) For Eurojust Staff Members managing the meeting (Back Office, Front Office, Co-Hosts[1])

• IP Address
• Hardware Type*
• Operating System Type and Version*
• Client Version*
• IP Addresses Along the Network Path*
• MAC Address of Client* (As Applicable)
• Service Version*
• Actions Taken
• Geographic Region – obtained from the IP address
• Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
• Number of Meetings**
• Number of Screen-Sharing and NonScreen-Sharing Sessions
• Number of Participants**
• Meeting Host Information:
    • Host Name
    • Meeting Site URL
    • Meeting Start/End Time
• Screen Resolution
• Join Method

*Data collected for Performance, Troubleshooting, and Diagnostics.
** Data collected for Analytics

3) For external participants joining a WebEx meeting

For VideoConferencing systems accessed by external participants via WebEx web browser plugin, smart phone app, or any other videoconferencing tool, the following personal data are collected:

• Email addresses (optional): this information is provided by the participant, and does not need to be their real email address
• IP address
• Username: this information is provided by the participant, and does not need to be their real name/surname.
• Phone numbers – only for those connecting via phone
• Device information*
• Hardware Type*
• Operating System Type and Version*
• Client Version*
• MAC Address of Client* (As Applicable)
• Service Version*
• Number of Meetings**

* Data collected for Performance, Troubleshooting, and Diagnostics

[1] A Co-host is the member of the organising Unit/Desk/Department in charge of managing the meeting

** Data collected for Analytics

3. Who has access to your personal data and to whom is it disclosed?

For the purpose detailed above, access to your personal data is given to the following persons, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with European Union law:

Access restrictions apply based strictly on need to know basis.

a) User Support
b) Back Office
c) For data listed in Section 1) and Section 2) above, and limited to the data indicated as to be collected for Performance, Troubleshooting, and Diagnostic: these data can be sent also the Cisco Technical Support, in charge of investigating and solving technical issues. In such case, a dedicated member of the Back Office Team will send the information to the Cisco Technical Support. Participants data listed under Section 3) will not be shared with Cisco Technical Support. Cisco Technical Support is located in several countries (as described in the attachment Cisco TAC Delivery Service Privacy Data Sheet). The data submitted to the Cisco Technical Support are stored on Amazon Web Services Data Centre located in North Virginia and are kept for 10 years.

4. How do we protect and safeguard your information?

The personal data collected by WebEx are encrypted as described below:

- Data listed in section 1) above are encrypted in transit.
- Data listed in section 2) above are encrypted in transit.
- Data listed section 3) above are encrypted in transit and at rest.
- All password listed under point 1), 2), 3), are encrypted in transit and at rest.

Additional information on the encryption methods are included in the attached Cisco Privacy Data Sheet.

5. How can you verify, modify or delete your information?

In case you wish to verify which personal data is stored on your behalf by the Controller, have it modified, corrected, or deleted, or restrict the processing, or object to it or to exercise the right to data portability, please make use of the following email address: usersupport@eurojust.europa.eu , by explicitly describing your request. Any correction of your personal data will be taken into consideration from the data protection point of view.

Identification data of individuals can be corrected at any time.

6. How long do we keep your personal data?

The retention period is the following:

Eurojust data described in section 1) above:

The data are maintained as long as an active subscription with Cisco is in place. In case of termination of service with Cisco, all the data are deleted with the exception of Name, UUID, and billing information which are kept are maintained for 7 years as part of Cisco's business record and to comply with Cisco financial and auditing policies.

Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years.

Eurojust data described in section 2) above

The data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust.

Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years.

Participants data described in section 3) above

The participants' data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust.

7. Contact information

You have the right to access, rectify or erase or restrict the processing of your personal data or, where applicable, the right to object to processing or the right to data portability in line with Regulation (EU) 2018/1725.

Any such request should be directed to the Controller, by using the following email address: usersupport@eurojust.europa.eu , and by explicitly specifying your request.

You may also contact the Data Protection Officer of the Eurojust (dpo@eurojust.europa.eu).

8. Recourse

You have the right to lodge a complaint to the European Data Protection Supervisor (https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data.

Annex

Cisco Webex Meetings

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Webex Meetings.

1. Overview of Cisco Webex Meetings Capabilities

Cisco Webex Meetings (the "Service" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who acquire it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding the People Insights and Facial Recognition optional features for Cisco Webex Meetings, please see the Addendums below. For a detailed overview of the Service, please visit the Cisco Web Conferencing homepage.

Because the Service enables collaboration among its users, as described below, your personal data is required in order to use the Service. The following paragraphs describe 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. Cisco will use your personal data consistent with this Privacy Data Sheet to serve the legitimate interests and fulfill the contractual obligations of providing the Solution. Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

2. Personal Data Processing

The Service allows users to instantly connect in a way that is almost as personal as a face-to-face meeting. If you are a user and your employer is the Customer that acquired the Service, your employer serves as the "data controller" for user generated content (see the Webex Meetings Privacy Data Map for a visualization of who is doing what with data). The information described in the table below and in this Privacy Data Sheet is accessible to your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. The meeting host has the option to record meetings, which may be shared with others or discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording and Webex displays a red circle visible to all participants indicating that the meeting is being recorded. Note, Cisco has no control over, and is not responsible or liable for the privacy of any information that you have shared with others. Even after you remove information from the Webex Meetings platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.

This Privacy Data Sheet covers the Cisco Webex Meetings Suite, Cisco Webex Events, and Cisco Webex Training. If you use the Service together with Cisco Webex Teams, see the see the Cisco Webex Teams Privacy Data Sheet (available on The Cisco Trust Center) for descriptions of the data that may be collected and processed in connection with those services. The table below list the categories of personal data used by the Service and describe why we process such data.

Personal data processing by the Service does not produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.

©2019 Cisco and/or its affiliates. All rights reserved.

Personal Data Category	Types of Personal Data	Purpose of Processing / Legitimate Interest
Registration Information	• Name • Email Address • Password • Public IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Geographic region • Avatar (Optional) • Billing Information • User information included in the Customer's Active Directory (if synched) • Unique User ID (UUID)	We use Registration Information to: • Provide you with the Service • Enroll you in the Service • Display your user avatar identity to other users • Make improvements to the Service and other Cisco products and services • Provide you support • Notify you about features and updates • Customer relationship management (e.g., transactional communication) • Authenticate and authorize access to your account • Bill you for the Service • Display directory information to other Webex users • Provide step-by-step guidance on how to use Webex online via WalkMe (optional)

Host and Usage Information	• IP Address
	• User Agent Identifier
	• Hardware Type
	• Operating System Type and Version
	• Client Version
	• IP Addresses Along the Network Path
	• MAC Address of Your Client (As
	• Applicable)
	• Service Version
	• Actions Taken
	• Geographic Region
	• Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
	• Number of Meetings
	• Number of Screen-Sharing and NonScreen-Sharing Sessions
	• Number of Participants
	• Meeting Host Information*
	  • Host Name
	  • Meeting Site URL
	  • Meeting Start/End Time
	• Screen Resolution
	• Join Method
	• Performance, Troubleshooting, and Diagnostics Information
	• Call attendee information, including email addresses, IP address, username, phone numbers, room device information
	
	* Used for billing purpose
		We use Host and Usage Information to:
		• Provide you with the Service
		• Understand how the Service is used
		• Diagnose technical issues
		Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
		• Respond to Customer support requests
		• Bill you for the Service
		• Make improvements to the Service and other Cisco products and services

User-Generated Information	• Meeting and Call Recordings • Transcriptions of Call Recordings • Uploaded Files (for Webex Events and Training only)	We use User-Generated Information to: • Provide the Service, optional components which include recording meetings

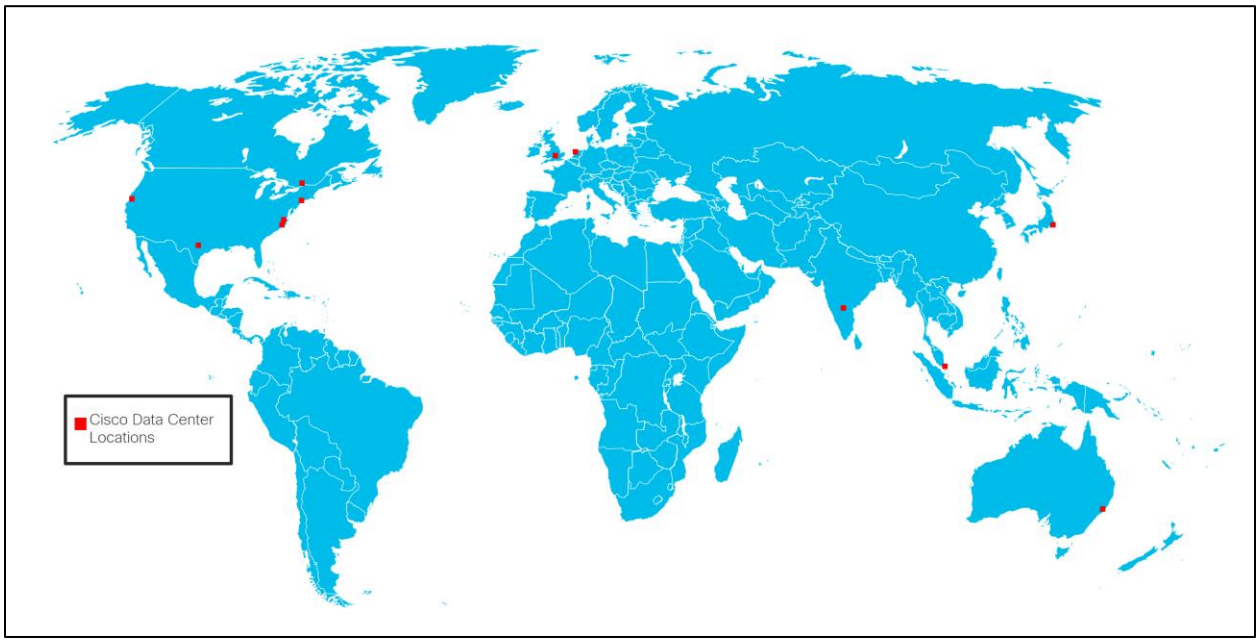
©2019 Cisco and/or its affiliates. All rights reserved.

Technical Support Assistance
If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

Webex Analytics Platform
Cisco Webex Control Hub Analytics provides usage trends and valuable insights that can be used to help with strategies to promote and optimize adoption across teams. The Webex Analytics Platform utilizes Registration, Host and Usage information to provide advanced analytics capabilities and reports.

3. Cross-Border Transfers

The Service leverages its own data centers to deliver the Service globally. If you join a meeting using Cisco Webex Teams, please see the Cisco Webex Teams Privacy Data Sheet for applicable privacy information, including data center locations. The Webex Meetings data centers are currently located in the following countries (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):



©2019 Cisco and/or its affiliates. All rights reserved.

Cisco Data Center Locations:	Internet Point of Presence (iPOP) Locations:
Amsterdam, Netherlands	Amsterdam, Netherlands
Bangalore, India	California, USA
California, USA	Hong Kong, China
London, UK	Illinois, USA
New York, USA	New Jersey, USA
North Carolina, USA*	Sydney, Australia
Singapore, Singapore	Texas, USA
Sydney, Australia	
Texas, USA*	
Tokyo, Japan	
Toronto, Canada	
Virginia, USA	

User-Generated Information is stored in the data center in Customer's region as provided during the ordering process. Data is replicated across data centers to ensure availability. Billing data is stored in Texas, USA and North Carolina, USA. Webex Analytics data is stored in California, USA and Texas, USA.

For free user accounts, the data defined in this privacy data sheet may be stored in a Webex data center outside the account holder's region. An Internet Point of Presence (iPOP) is used to route traffic geographically from nearby areas to a Cisco Data Center Location. It is intended to route Webex Meeting traffic through Cisco's infrastructure and improve performance. Data routed through these internet point of presence points remains encrypted and is not stored.

Please see the Webex Meetings Privacy Data Map for a visual representation of the data flows.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- EU Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- EU Standard Contractual Clauses
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors

©2019 Cisco and/or its affiliates. All rights reserved.

4. Access Control

Customers and Cisco can access personal data on the Service as described in the table below.

Personal Data Category	Who has access	Purpose of the access
Registration Information	User through the My Webex Page	Modify, control, and delete information
	Customer through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Host through the My Webex Page	View meeting session Information
	Customer may view this information through the Site Admin Page, Webex Control Hub, or may be otherwise provided by Cisco	View usage, meeting session and configuration information
	Cisco	Support and improvement of the Service by the Cisco Webex Meetings support and development team
User Generated Information	User through the My Webex Page	Modify, control, and delete based on user's preference
	Customer using APIs provided with the Service or through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access in accordance with Cisco's data access and security controls process.
	Other Customers and users (when shared during a meeting)	Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

5. Data Portability

The Service allows Customers and users to export all User-Generated Information. A Customer's administrator may do so using APIs provided with the Service (recordings only) or through the Site Admin Page; while individual users may do so through the My Webex Page. Meeting recordings are available in proprietary ARF and standard mp4 formats depending on the account type. Cisco offers a free ARF player to convert ARF files to mp4 format.

Customers are permitted to export personal data collected about their users on the Webex Meetings platform using APIs or via the Site Admin Configuration.

©2019 Cisco and/or its affiliates. All rights reserved.

6. Data Deletion & Retention

Subject to their employer's corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the My Webex Page at any time during the term of their subscription. Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. Cisco provides free account users up to 6 months of free storage.

Customers can request deletion of other personal data retained on the Webex Meetings platform by sending a request to Cisco (see contact options in Section 11 below) or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes or other legal requirement, Cisco endeavors to delete the requested data from its systems within 30 days. The table below describes the retention period and the business reasons that Cisco retains the personal data. Users seeking deletion of other personal data retained on the Webex Meetings platform must request deletion from their employer's site administrator.

Personal Data Category	Retention period	Reason and Criteria for Retention
Registration Information	Active Subscriptions: • Registration Information will be maintained as long as Customer maintains active subscription (paid or free). Terminated Service: • Deleted once the Service is terminated • Name and UUID are maintained 7 years from termination	Name and UUID are maintained 7 years from termination as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing information is also subject to this retention period.
User Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: • Deleted within 60 days	User-Generated Information is not retained on the Webex Meetings platform when Customer or user deletes this data.
Host and Usage Information	3 years from when the Service is terminated*	Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery. Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized. Once the specified retention period has expired, data will be deleted or anonymized. * Any billing information is retained for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements.

7. Personal Data Security

The Service adopts technical and organizational security measures designed to protect your personal data from unauthorized access use or disclosure. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Type of Encryption
Registration Information (excluding Passwords, discussed below)	Encrypted in transit, but not at rest
Passwords	Encrypted and hashed in transit and at rest
Host and Usage Information	Encrypted in transit, but not at rest
User Generated Information	Recordings prior to May 2018 were encrypted in transit with the option to encrypt at rest. Recordings created after May 2018 are encrypted in transit and at rest by default. Recordings created in the Webex Meetings FedRAMP-Authorized service after October 2019 are encrypted in transit and at rest.

©2019 Cisco and/or its affiliates. All rights reserved.

Protecting Data at Rest

The Service encrypts sensitive data at rest. Any data not encrypted at rest is protected by highly-secure data center protection mechanisms and operational procedures. Webex Meetings data centers feature communication infrastructure with industry-leading performance, integration, flexibility, scalability, and availability.

Encryption at Run Time

All communications on the Webex Meetings platform occur over encrypted channels. After a session is established, all media streams (audio, VOIP, video, screen share, and document share) are encrypted. The Service then re-encrypts the media stream before sending it to other users. Note that if a Customer allows attendees to join its meetings using third-party video end points, those attendees may be sending your meeting data unencrypted on the Internet. Media streams flowing from a user to Cisco Webex Meetings servers are decrypted after they cross the Cisco firewalls. This enables Cisco to provide network-based recording and SIP-based call support for video end points.

End-to-End Encryption (Optional)

For businesses requiring a higher level of security, the Service also provides end-to-end encryption. With this option, the Service does not decrypt the media streams. In this model, traffic cannot be deciphered by the Cisco Webex Meetings server. The end-to-end encryption option is available for Webex Meetings and Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported:

- Network-based recordings
- Join Before Host
- Cisco Webex Video Platform (formerly known as Collaboration Meeting Rooms Cloud)

8. Third Party Service Providers (Sub-processors)

We share Registration Information, Host Information, and/or Usage Information with service providers, contractors or authorized third parties to assist in providing and improving the Service. We do not rent or sell your information. The data shared may include aggregate statistics, de-identified, or pseudonymized data. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. Below is a list of sub-processors for WebEx Meetings.

Sub-processor	Personal Data	Service Type	Location
Amazon Web Services (AWS)	Limited Host & Usage Information, meeting media traffic	AWS cloud infrastructure is used to host the Webex signaling service that processes real-time meeting lifecycle information such as meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (location maps to Customer's Webex data center assignment) AWS cloud infrastructure is used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended.	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore
WalkMe* *Feature will be enabled for Enterprise sites in June 2020, Customers may turn this feature off at any time. Feature is currently enabled for non-enterprise Webex sites.	Unique User ID (UUID) and user region	Provides user with a step-by-step tour and guidance on how to use Webex Meetings online site.	Globally

©2019 Cisco and/or its affiliates. All rights reserved.

If a Customer acquires the Service through a Cisco partner, we may share any or all of the information described in this Data Sheet with the partner. Customers have the option of disabling this information-sharing with Cisco partners. If you use a third-party account to sign-in to your Webex account, Cisco may share only the necessary information with such third party for authentication purposes.

9. Information Security Incident Management

Breach and Incident Notification Processes
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.

10. Certifications and Compliance with Privacy Laws

The Security & 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. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements, including the EU General Data Protection Regulation, California Consumer Privacy Act, Canada's Personal Information Protection and Electronic Documents Act and Personal Health Information Protection Act.

Cisco leverages the following privacy certifications to demonstrate alignment with global privacy frameworks and transfer mechanisms related to the lawful use of data across jurisdictions:

- EU Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- EU Standard Contractual Clauses
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. The Service has received the following certifications:

- ISO 27001, 27017, and 27018
- SOC 2 Type II Attestation, SOC 3, + C5
- FedRAMP

11. How to Exercise Your Data Subject Rights

You have the right to request access, rectification, suspension of processing, or deletion of your personal data processed by the Service.

©2019 Cisco and/or its affiliates. All rights reserved.

We will ask you to confirm your identification (typically with the email address associated with your Cisco account) before responding to your request. If we cannot comply with your request, we will provide you with an explanation. Please note, if you are a user and your employer is the Customer/Controller, we may redirect you to your employer for a response.

Requests can be made by the following means:

1) sending an email to privacy@cisco.com
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost
NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to your inquiries and requests. If you have an unresolved privacy concern related to the personal data processed or transferred by Cisco, you may contact Cisco's US-based third-party dispute resolution provider by clicking here. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

12. General Information and GDPR FAQ

For more information related to technical and operational security features of the Service, please see the Webex Meetings Security White Paper and the Cisco Webex Trusted Platform site.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.

©2019 Cisco and/or its affiliates. All rights reserved.

Addendum One: People Insights feature for Cisco Webex (Optional)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the People Insights feature for Cisco Webex Meetings and Cisco Webex Teams.

1. Overview of People Insights Capabilities

The People Insights feature ("People Insights" or the "Feature") provides Cisco Webex users with comprehensive, publicly available business and professional information for meeting participants giving users context and increased insight about the people with whom they collaborate.

Only the Customer's site administrator has the ability to enable the Feature for their organization and users. Individual users cannot opt-in to use People Insights independently of their site administrator. Users at an enabled organization can opt-out of People Insights by suppressing their profile from other meeting participants' view. This is accomplished in two ways:

1. Entering a meeting and selecting the "Hide Profile" link,
2. Signing into people.webex.com and clicking on "Hide Profile"

2. Personal Data Processing

People Insights compiles business and professional profiles for meeting participants using publicly available and legitimately sourced information, published authored works, news articles, search engine results, via APIs and through content supplied by the profile owner.

The tables below list the personal data used by People Insights and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Publicly Available Business and Professional Biographical Data	• Profile Photos • News • Tweets • Authored Works • Bios • Employment History • Education History • Web Links for a specific person	• To source the People Insights profile and to enable search within the feature.
Account & Usage Information	• User Level Account Details (including email, name, and web interactions and platform usage)	• To provide support and improvement of the Feature • Product analytics (e.g. frequency of profile edits, # of successful profile loads in a meeting, etc.)

©2019 Cisco and/or its affiliates. All rights reserved.

Personal Data Category	Types of Personal Data	Purpose of Processing
Directory Data	• If the Active Directory option is enabled by the site administrator, professional information including the following may be collected from the internal company directory (as selected by the site administrator): • Title • Phone Number • Location • Organization • Department • Photo • Role • Reporting Structure	• To augment the user's People Insights profile by providing company specific context to meeting participants who belong to the same organization. This data will only be visible to participants within the user's organization.
User Generated Information	• Information that the user adds in their People Insights profile.	• Augment the user's own People Insights profile (visible to Insights users)

3. Cross-Border Transfers

People Insights data is stored on third party servers provided by Amazon Web Services ("AWS") and Algolia. AWS servers are located in Oregon, Ohio and Virginia. Algolia servers are located in California.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings or Teams Privacy Data Sheets.

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Publicly Available Business and Professional Biographical Data	Customer Cisco People Insight users within the Customer's organization	To provide the Feature
Account Information	Cisco	Registration Support Correlate users with correct profiles Analytics to improve service
	Customer	Feature enablement/disablement.
Customer Directory Data	Customer (Admin) People Insight users within the Customer's organization	Directory data is provided and maintained by customer administrator to allow integration into People Insights profile.
	Cisco	Directory data is imported and integrated with customer profile data to support profile development
User-Generated Information	User	Users may access their own User-Generated Information to edit or delete content.

5. Data Portability

Individuals can receive a copy of their own People Insights profile, including their self-generated information, by contacting privacy@cisco.com

©2019 Cisco and/or its affiliates. All rights reserved.

6. Data Deletion & Retention

Type of Personal Data	Retention Period	Criteria for retention
Publicly Available Business & Professional Data	Obtained from public websites: Indefinite Obtained through third-party APIs: In accordance with contractual requirements	Publicly Available Business & Professional Data is derived from public sources. It is retained indefinitely by default. Upon request, publication and links to source data can be suppressed and restricted from view and publication. As publicly available data originates from outside of Cisco WebEx, any permanent changes or deletions must be addressed and requested with the primary source. At the request of users, the data can be archived in order to not appear. This allows for the data to remain permanently hidden rather than re-appearing with a new search after being previously purged.
Account Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within 30 days.
Directory Data	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Administrators can disable Active Directory feature while still enabling People Insights. Directory data will be hard deleted in this case of deactivation. Non-directory data will remain, with the exception of name and email for users who had only directory data in their profile before the deactivation.
User-Generated Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can delete User-Generated Information from their profile at any time.

7. Personal Data Security

Personal Data Category	Type of Encryption
Publicly Available Business & Professional Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
Host & Usage Information	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
Directory Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
User-Generated Information	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for People Insights is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	Oregon Ohio Virginia
Algolia	• Publicly Available Business and Professional Biographical Data	Full Text Search	California
Amplitude	• Host & Usage Information	User Analytics	California

©2019 Cisco and/or its affiliates. All rights reserved.

Addendum Two: Facial Recognition feature for Cisco Webex Meetings (Optional)

This addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Facial Recognition feature for Cisco Webex Meetings.

1. Overview of Facial Recognition Capabilities

Cisco introduced the facial recognition feature ("Facial Recognition" or the "Feature") to provide Webex Meetings users with the ability to identify and recognize registered Webex meeting participants (i.e., associate participant names with their positions in a Webex meeting video), giving users increased connection to meeting participants. The Feature recognizes a face by converting it to an abstracted facial vector. A facial vector is a list of numbers that characterize salient facial features of a user that is then used to identify who is in the meeting. This level of abstraction allows the system to recognize the same face even when things like lighting and position change.

Facial Recognition is disabled by default, and requires affirmative action by both the customer and the user to enable. First, the administrator for the customer may enable Facial Recognition using Webex Control Hub. However, the feature will not be available on the user's account until the user opt-ins at https://settings.webex.com. Because the Feature is based on facial vectors derived from profile images, the user must have a picture taken at the time of enablement.

2. Personal Data Processing

If the user opts-in to the Facial Recognition feature, the web page uses the camera of the user's device to take a profile picture. This picture is sent to the Webex cloud where the Feature algorithm generates a facial vector from the picture so that it can be used for matching as further described below. Both the picture and the facial vector are encrypted and stored securely. The picture may be used to generate a new facial vector in the event Cisco updates or modifies the algorithm by which facial vectors are generated. In the event a customer or user reaches out to Cisco for support with the Feature, Cisco may also use the picture during the troubleshooting process. During each meeting, a second facial vector is generated, then matched in the Webex cloud against the stored facial vector. This second facial vector is not retained.

The tables below list the personal data used by the Feature and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration	• Name (First, Last) • Email • User ID	• To display name of recognized user • Enroll you in the Feature and enable opt-in
Biometrics	• User facial image • Facial vector mapping	• To create facial vector mapping and provide the facial recognition feature • To generate a new facial vector in case of a modification or update to the Feature algorithm • To provide the Facial Recognition feature

Host & Usage Information	• Information regarding accuracy of product, including:
	  ○ Successful and unsuccessful facial vector matching
	  ○ User feedback
		• To provide support and product analytics

Location	• Meeting Room Proximity data	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

©2019 Cisco and/or its affiliates. All rights reserved.

Personal Data Category	Types of Personal Data	Purpose of Processing
Calendar	• Meeting Room Calendar Information	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

3. Access Control

Personal Data Category	Who has access	Purpose of the access
Registration	Cisco	• To display name of recognized user • Enroll you in the Feature and enable opt-in
	Customer	• View user facial recognition registration status
	Users through https://settings.webex.com/	• View and modify facial recognition registration details
Biometrics	Cisco	• To provide the Facial Recognition feature • Algorithm improvement • To troubleshoot issues in the event a customer or user requests support • To provide the Facial Recognition feature
Host & Usage Information	Cisco	• To provide support and product analytics
Location	Cisco	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	Cisco	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

4. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the automatic export of Facial Recognition data.

5. Data Deletion & Retention

Type of Personal Data	Retention Period	Reason and Criteria for Retention
Registration	User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Facial Recognition service. All other registration information is not stored or retained by the Facial Recognition service as this information is already stored by Webex Meetings.	UserID is used to track your enrollment in the Feature Names are displayed upon a match in the facial recognition feature.

©2019 Cisco and/or its affiliates. All rights reserved.

Type of Personal Data	Retention Period	Reason and Criteria for Retention
Biometrics	Images: Users control their image retention. The image is retained as long as the feature is enabled and the user leaves the image associated with their profile. The image can be deleted at any time by user. Images for all users are deleted upon customer's discontinuation of the service.	The image is used to provide the Facial Recognition feature, update the facial vector in case of an update to the algorithm, and to troubleshoot issues when requested by a customer or user.
	Facial vectors are retained as long as the facial images, but are stored separately. Facial vectors are deleted upon discontinuation of the service.	The facial vectors are used to provide the facial recognition feature.
Host & Usage Information	2 Weeks	To provide support and product analytics
Location	2 days	Proximity data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.
Calendar	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	Calendar data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.

6. Personal Data Security

The table below summarizes encryption architecture of data stored specifically for the Facial Recognition feature.

Personal Data Category	Type of Encryption
Registration	Encrypted in transit, AES 256 for storage
Images	Encrypted in transit, AES 256 for storage
Biometrics	Encrypted in transit, AES 256 for storage
Host & Usage Information	Encrypted in transit, AES 256 for storage
Location	Encrypted in transit, AES 256 for storage

©2019 Cisco and/or its affiliates. All rights reserved.

Addendum Three: Webex Assistant for Meetings (Optional)

This addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the Webex Assistant for Meetings ("Webex Assistant" or "Assistant") feature for Cisco Webex Meetings.

1. Overview of Webex Assistant Capabilities

Webex Assistant for Meetings is an intelligent, interactive virtual meeting assistant that makes meetings searchable, actionable, and more productive. When Webex Assistant is turned on, the meeting host and participants can capture meeting highlights with one click or through a voice command. Even when Webex Assistant joins a Meeting, it will only be activated by the wake word, "OK Webex." Once the wake word is detected, the voice command is streamed to the cloud for speech-to-text transcription and processing. Any participant can use one of many voice commands and create a meeting highlight. Meeting Highlights can include meeting key points, notes, summaries, agendas, action items or decisions. Webex Assistant can also show captions so that no one misses a word of what's being said. Additionally, a meeting host can record the meeting to get a post-meeting transcript.

Webex administrators can provision Webex Assistant for Meetings for an organization, an entire Webex site, or for specific users through license assignment. A Customer's administrator can enable and disable Webex Assistant at any time. The administrator may also set the Assistant default to be either ON or OFF at meeting start times. If the Assistant is set to default ON by an administrator, the Assistant will be on when the meeting begins but can be disabled. If Assistant setting is set to OFF, the meeting host will have to explicitly turn on the Assistant in the meeting in order to use it.

Cisco has put several controls in place to ensure user transparency. When Webex Assistant is enabled, the Webex Assistant icon appears in the lower left of the host and participant's screen. On Webex endpoint devices, there will be a visual cue similar to the existing one you see when a meeting is recorded. Additionally, when the host turns on Webex Assistant in a meeting, there will be an audio announcement made to all participants on the call, even if they join late. As further described below, the host can choose to share the transcript and meeting highlights with other Webex Meeting users.

2. Personal Data Processing

The tables below list the personal data used by the Feature and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • Username • Unique User Identifier (UUID)	• Provision Webex Assistant licenses to specific Webex Meeting users or to an entire organization or site • Provide the Webex Assistant service
Audio Information	• Meetings Recordings • Audio Commands to Webex Assistant • Audio associated with meeting Highlight	• Provide the Webex Assistant Service
Transcript Information	• Meeting Transcript • Text of meeting Highlight	• Provide the Webex Assistant service

©2019 Cisco and/or its affiliates. All rights reserved.

Personal Data Category	Types of Personal Data	Purpose of Processing
Host and Usage Information	• Usage of the Webex Assistant features, including number of meetings with Assistant enabled, number/type of Highlight views/edits/downloads, troubleshooting events	• Provide the Webex Assistant service • Understand how the service is used • Provide Customer with usage information • Diagnose technical issues • Improve the technical performance of the service

3. Access Control

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	Enroll the to the Webex Assistant service.
	Customer	Provision Webex Assistant licenses to specific Webex Meeting users or to an entire organization or site
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.
	Customer	Customer will continue to have access to Meeting Recordings in accordance with Customer's personal data policy and as described in the Meetings Privacy Data Sheet.
	User	A meeting host will be able to view, access and/or delete Highlights. A host may share and give certain edit permissions to other Webex Meetings users.
Transcript Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	A meeting host will be able to view, access and/or share Transcript Information. A host may share and give certain edit permissions to other Webex Meetings users.
Host and Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.

©2019 Cisco and/or its affiliates. All rights reserved.

4. Cross Border Transfers

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service globally. Webex Assistant Audio and Transcript Information will be stored in the same location in which the Customer is provisioned for Webex Meeting recordings. Although Webex Assistant may process data in AWS as listed in Section 8 below, no data will be stored there.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings privacy data sheet.

5. Data Portability

Users have the option to email any transcript or Highlight to a selected email account.

6. Data Deletion & Retention

Subject only to their employer's corporate retention policies, users with an active subscription have control over their Audio and Transcript Information and can delete such information from their account through the My Webex Page as described below. If you have any questions regarding deletion or deletion requests, please email privacy@cisco.com.

Type of Personal Data	Retention Period	Reason and Criteria for Retention
User Information	User Information is not separately stored or retained by the Webex Assistant service as this information is already stored by Webex Meetings.	User Information is not separately stored or retained by the Webex Assistant service as this information is already stored by Webex Meetings.
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained in order to provide you with the service and will be deleted once it is no longer necessary to provide the service.
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained in order to provide you with the service and will be deleted once it is no longer necessary to provide the service.
Host and Usage	Deleted after 3 years.	Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

©2019 Cisco and/or its affiliates. All rights reserved.

7. Personal Data Security

The table below summarizes encryption architecture of data stored specifically for Webex Assistant.

Personal Data Category	Type of Encryption
User Information	Webex Assistant does not store or retain this information separately than already maintained by Webex Meetings.
Audio Information	Encrypted in transit, and at rest.
Transcript Information	Encrypted in transit, and at rest.
Host and Usage	Encrypted in transit, and at rest.

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Webex Assistant is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, Germany, Singapore
Google Cloud	Audio and transcript of Voice Command *only* (e.g., "Ok, Webex, ***create a note***"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech to Text service (voice commands only) • Text to Speech service (voice command responses only)	US, Germany, Singapore

©2019 Cisco and/or its affiliates. All rights reserved.

Cisco Webex Control Hub (Data Security and Privacy) Data Sheet

Updated: October 2, 2020

Data security and privacy overview

One of the key benefits for enterprises of consuming cloud services is the ability to leverage value-added features and functionality as quickly as the cloud service provider can deploy them. But for many cloud providers, “adding value” often means having full access to user data and content. For collaboration applications, most cloud providers directly access message, call, and meeting content in order to offer features such as message search, content transcoding, and integration with third-party applications. On the other hand, modern consumer collaboration services tend to be geared toward protecting consumer privacy by offering end-to-end encryption at the expense of features that add value.

Cisco Webex® provides the best of both worlds: an end-to-end encrypted cloud collaboration platform that offers enterprises the ability to choose which, if any, of the value-added integrations Cisco and third parties provide. Webex uses an open architecture for the secure distribution of encryption keys, allowing enterprises to gain control over the management of their encryption keys and the confidentiality of their data. This means that content is encrypted on the user’s Cisco Webex Teams app and remains encrypted until it reaches the recipient, with no intermediaries having access to decryption keys for content unless the enterprise explicitly chooses to grant such access.

The impact of breaches can be severe, and so Cisco has introduced integrations and controls into its Webex portfolio to allow customers to manage the application of their security policies. Cisco® Webex Control Hub is a web-based, intuitive, single-pane-of-glass management portal that enables you to provision, administer, and manage Webex services.

The Pro Pack for Webex Control Hub is a premium offer for customers that require more advanced capabilities and integrations with their existing compliance, security, and analytics software.

Webex security differentiation

- Webex baseline security for user-generated data is among the strongest in the collaboration solutions market. Frequently, other collaboration vendors provide security through piecemeal encryption of data during transit, while at rest on devices, and during storage—all using different solutions. No enterprise messaging offer today supplies the true end-to-end encryption provided by Webex Teams.
- Customers’ ability to hold keys on-premises (using Webex Hybrid Data Security or HDS) also differentiates Webex from the competition, because customers can not only manage their key

storage, but also host key compliance and search services on-premises. HDS handles unencrypted content for compliance and search services in the customer's secure data centers instead of on the Webex platform.

- The Webex platform always stores encrypted content in a realm separate from the storage of keys and services that handle unencrypted content. Despite having achieved this level of data security, Webex has not compromised on enterprise-grade features such as content searches, e-discovery, archival capabilities, and Data Loss Prevention (DLP).

Webex data security using cloud key management services

Webex platform-based Key Management Services (cloud KMS) are available by default to all customers to encrypt their content before it leaves a user's Webex Teams™ app. This baseline for all customers, including online offer consumers, helps ensure that Cisco always provides KMS and end-to-end encryption.

With cloud KMS, every Webex Teams users get:

- Clear separation between the services that handle storage and transport of encrypted content and the services that handle encryption and security key management
- An end-to-end encrypted channel between the cloud KMS and the Webex Teams app or Webex registered device for exchanging keys
- Industry-standard encryption of user-generated content using symmetric keys managed by the cloud KMS (minimum of one key per Webex Teams space)
- Controlled authorization to access keys using users' access tokens
- Encrypted search capabilities
- Enterprise capabilities such as e-discovery, DLP APIs, and archival capabilities, with decryption done at the perimeter, authorized by the administrator

Webex data security with Hybrid Data Security

Security-conscious enterprise customers may choose to deploy the security realm services, including KMS, on their own premises. This works no differently than using the cloud KMS, except that keys are obtained and accessed through an on-premises deployment of the servers.

Hybrid Data Security (HDS) includes:

- On-premises deployment and management of the security realm through the Pro Pack for Webex Control Hub
- KMS and storage
- Deployment that supports both inspecting and non-inspecting for both transparent and explicit proxies, including the mode where external DNS resolution is blocked
- Search indexer: Ability to securely search encrypted Webex Teams content
- E-discovery on-premises engine: Although the e-discovery user interface will be hosted in the

cloud, the engine remains on the premises for customers who opt to deploy HDS in their own data centers

- Automatic upgrades, alerts, and notifications
- Local logs and audits of access to keys using an on-premises “bring-your-own” syslog

Webex data security features

Table 1 summarizes Webex data security features.

Table 1. Data security features

Feature	Standard offer/ Pro Pack required	Description
End-to-end encryption of content Note: Includes user-generated content such as messages, file uploads, space names, meeting subjects, device nicknames, and Cisco Webex Board content	Standard offer	Webex Teams uses industry-leading encryption to help ensure that Webex messages, files, and whiteboards remain confidential, available, and secure at all times. The Webex Teams application encrypts your data before it leaves your device, using dynamic keys from the KMS. Data stays encrypted when it's in transit to our cloud servers, when we process your data (data in use), and when we store it (data at rest). The KMS is responsible for creating, maintaining, and authorizing access to the encryption keys that the Webex Teams app uses to encrypt and decrypt content.
Encryption in transit	Standard offer	We use secure HTTPS for all web transactions between Webex Teams for Mac, Windows, iPhone, Android, and web and our cloud. Similarly, HTTPS is used for all web transactions from Webex devices (for example, Webex room devices, IP phones, Webex Board). Web APIs on the Cisco® Collaboration Cloud (at developer.webex.com) use HTTPS. There is no support for HTTP. Consequently, all transport in and out of the Cisco Collaboration Cloud is encrypted. HTTPS is also used to protect data in transit from or to Webex Control Hub. All media in Webex, such as voice, video, desktop share,

Feature	Standard offer/ Pro Pack required	Description
		and whiteboarding, are transmitted using Secure Real-Time Transport Protocol (SRTP, defined in RFC 3711). Currently, the Webex platform decrypts real-time media for mixing, distribution, PSTN trunking, and demarcation purposes.
Search on encrypted content	Standard offer	Search indexes for all user-generated messages are created when encrypted content is received in the Cisco Collaboration Cloud. Search indexes are one-way hashed using dynamic keys before being stored. When the end user searches for a word in Webex Teams, the word is encrypted before leaving the app. Words are appropriately hashed and searched against previously stored encrypted search words. Matches are retrieved and sent to the app for decryption and display to the end user.
Hybrid Data Security (customer-controlled data security)	Pro Pack required	Enterprises can opt to deploy both the services that manage and store the keys used for encrypting content and the services that generate search index hashes. The deployment supports both inspecting and non-inspecting for both transparent and explicit proxies, including the mode where external DNS resolution is blocked. With these capabilities, enterprise customers have the additional assurance of choosing the location where their users' keys are physically stored. This capability, once it is deployed, should be run in a trial mode first for a select set of users, to help ensure a smooth rollout of the service. More details can be found in the deployment guide.

Frequently asked questions

Q. What encryption algorithm is used for encrypting content?

A. The symmetric cipher used to encrypt Webex Teams content is AES-256 GCM.

Q. Is there an Internet Engineering Task Force (IETF) protocol defined for KMS?

A. Webex builds on open standards and protocols for securing data, including key management specifications designed by Cisco and openly submitted for consideration as Internet standards.

Q. How can I obtain HDS?

A. HDS is one of the many features available for purchase as part of the Pro Pack for Webex Control Hub.

Q. Is a detailed deployment guide available for HDS?

A. Please see https://www.cisco.com/go/hybrid-data-security

Q. What additional security does HDS guarantee?

A. HDS gives you physical control of the keys that are generated and owned by your organization. Although certain cloud services can access those keys, separating the keys from the encrypted content in the cloud assures security-conscious organizations that their content cannot be compromised by outside attacks unless the attacker can access both the encrypted content and the keys.

Application and mobile device security controls

Overview

The Cisco Webex Teams application is enterprise-grade, and Cisco is committed to meeting customer security needs with the Webex platform. Enterprise IT requires basic controls on the security of the applications it deploys to users. With Webex Teams, the available controls include capabilities such as PIN lock enforcement, token revocation and remote wipe of Webex Teams cached content on mobile devices, and Webex Teams for Web idle session timeout.

Reset access

In the user profile, an administrator has the ability to revoke the user's access. This will remove all access and refresh the tokens of that user and will also remotely wipe all cached content on the mobile devices that the user is authenticated into. The typical use cases for this capability are when a user loses a mobile device or when a user is terminated but not yet deprovisioned from Webex.

Mobile device security controls

The Cisco Webex Teams for iPhone and Android apps benefit from the following enterprise-grade security features:

- All supported Webex authentication – password based or single sign-on based – establishes OAuth tokens for authorizations. Once established, the client refreshes the access tokens, never requiring a reauthentication unless specific events such as deprovisioning or token revocation occur.
- End-to-end encryption using dynamic keys.
- Secure Transport Layer Security (TLS) connection to the Cisco Webex service and to the user's organization-defined KMS (Cisco Webex platform or HDS).
- PIN lock requirement when enabled (Pro Pack required). This capability requires users to secure their devices with PIN lock or passcode, helping ensure that enterprise content in the Webex Teams app is not accessible if the device is misplaced, lost, or in the wrong hands.

- Remote wipe of content cached on mobile devices when either the user is deprovisioned from Webex or the user's access tokens are revoked by an administrator.
- Encryption at rest on Webex Teams for mobile apps.
- Basic Mobile Device Management (MDM) support certified with Cisco Meraki® Systems Manager and AirWatch, but not limited to these providers.

Webex application and mobile device security features

Table 2 summarizes the application and mobile device security controls.

Table 2. Application and mobile device security control features

Feature	Standard offer/ Pro Pack required	Benefit
PIN lock enforcement Note: Only for iOS and Android smartphones; does not include Chromebook	Pro Pack required	Once enabled by an enterprise administrator, PIN lock enforcement requires the user of Webex Teams for iPhone and Android to enable the device's PIN lock when using certain features in the mobile app, in order to continue using the app. This feature helps ensure the security of the content in the Webex Teams app.
Remote wipe and access reset by administrator	Pro Pack required	When a user loses their mobile device or has left the organization, an administrator can revoke all access and wipe Webex Teams cached content from the mobile device (iPhone and Android), helping ensure content security for the enterprise.
File share controls	Pro Pack required	An enterprise can choose not to use Webex file shares if there is concern for data leaks or they have other file management vendors for compliance or regulatory reasons.
Basic MDM support	Standard offer	Webex Teams mobile apps can be managed through MDM providers and security controls enabled for the device to protect data leaks or exfiltration. • Disable copy/paste, backups, document sharing.

Feature	Standard offer/ Pro Pack required	Benefit
		• Enforce device-level passcode and remote wipe. Note: This support is specifically verified with Meraki Systems Manager and VMware AirWatch, but the basic controls are expected to work with most MDM providers.
External communication control	Pro Pack required	An Enterprise can choose not to allow external communication due to information security and data loss concerns. As a result, users within the org cannot add users outside the org in spaces owned by the org and users within the org will not be able to join external spaces. Guest meetings and calls will still be allowed.

Frequently asked questions

Q. Is Cisco Webex certified for specific MDM providers?

A. Yes.

Q. How can an administrator access the PIN lock enablement feature?

A. This is a premium feature enabled through the Pro Pack for Webex Control Hub. It becomes available under Settings when you purchase the add-on offer.

Q. Will more security controls be added?

A. Yes. Webex is a cloud service and will constantly be adding new features to help ensure ongoing control and visibility.

Endpoint connectivity

Cisco Webex supports seamless connectivity to the cloud through already deployed proxies. Authentication types supported include NoAuth, Basic, and NTLM for mobile and desktop clients, digest-based authentication for mobile clients, and TLS intercept proxy on desktop clients. Proxy configuration methods supported are manual configuration, Proxy Auto-Config (PAC), and Web Proxy Auto Discovery (WPAD). Group Policy Objects (GPO) are supported only on Windows clients.

With the proxy support now available with Webex, proxy allowed listing is no longer necessary. For

network requirements to enable proxy support, please see the following two articles:

Network Requirements for Cisco Webex: https://collaborationhelp.cisco.com/article/en-us/WBX264

Network Requirements for Cisco Webex Teams Services: https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Certifications and regulatory compliance

Cisco Webex has an impressive set of standard certifications and is in compliance with many of the international regulations, allowing Webex to be sold across the globe (Figure 1). These certifications and regulations are as follows:

- ISO/IEC 27001, 27017
- ISO 27018
- SOC 2 Type 1 and Type 2
- Cloud Computing Compliance Controls Catalogue (C5)
- HIPAA compliant for use by healthcare customers through a HIPAA Self-Assessment
- FedRamp for Meetings
- EU-US Privacy Shield
- Swiss-US Privacy Shield
- APEC Cross Border Privacy Rules
- Binding corporate rules
- EU Model Clauses
- EU GDPR

Data locality

Cisco Webex provides the option for European customers to choose to provision their user identities and encryption keys in European data centers. View the data locality overview for more details. Cisco Webex certifications and regulatory compliance

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Cisco Webex Meetings Security

Introduction

Cisco Webex® Meetings helps enable global employees and virtual teams to collaborate in real time as though they were working in the same room. Businesses, institutions, and government agencies worldwide rely on Cisco® Webex Meetings solutions. These solutions help simplify business processes and improve results for sales, marketing, training, project management, and support teams.

For all these companies and agencies, security is a fundamental concern. Online collaboration must provide multiple levels of security for tasks that range from scheduling meetings to authenticating participants to sharing documents.

Cisco makes security the top priority in the design, development, deployment, and maintenance of its networks, platforms, and applications. You can incorporate Cisco Webex Meetings solutions into your business processes with confidence, even with the most rigorous security requirements.

This paper provides details about the security measures of Cisco Webex Meetings and its underlying infrastructure to help you with an important part of your investment decision.

Note: The terms "Cisco Webex Meetings" and "Cisco Webex Meetings sessions" refer to the integrated audio conferencing, Internet voice conferencing, and video conferencing used in all Cisco Webex Meetings online products. Unless otherwise specified, the security features we describe pertain equally to all the Cisco Webex Meetings applications listed in this paper.

What you will learn

This paper describes the security features of Cisco Webex applications and related services. It discusses the tools, processes, and engineering that help customers confidently collaborate on the Cisco Webex Meetings platform.

Cisco Webex Meetings applications include:

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support (including Cisco Webex Remote Access)
- Cisco Webex Edge
- Cisco Webex Cloud Connected Audio

© 2020 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco Webex Security Model

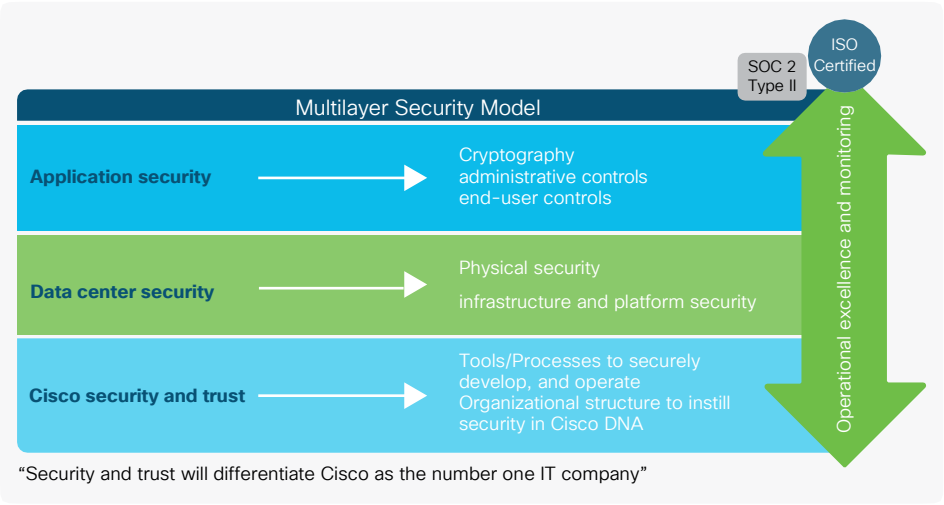
Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout our company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet the highest levels of security in everything we do.

This organization is also dedicated to providing our customers with the information they need to mitigate and manage cybersecurity risks.

The Cisco Webex security model (Figure 1) is built on the same security foundation deeply engraved in Cisco's processes.

The Cisco Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Cisco Webex services. We will be discussing some of these elements in this document.

Figure 1. Cisco Security Model



"Security and trust will differentiate Cisco as the number one IT company"

Cisco Security and Trust

Cisco security tools and processes

Cisco secure development lifecycle

At Cisco, security is not an afterthought. It is a disciplined approach to building and delivering world-class products and services from the ground up. All Cisco product development teams are required to follow the Cisco Secure Development Lifecycle. It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Cisco Webex Product Development team passionately follows this lifecycle in every aspect of product development.

Read more about the Secure Development Lifecyle.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco foundational security tools

The Cisco Security and Trust organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development.

Some examples of tools include:

- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling
- Coding guidelines
- Validated or certified libraries that developers can use instead of writing their own security code
- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects
- Software tracking that monitors Cisco and third-party libraries and notifies the product teams when a vulnerability is identified

Organizational structure that instills security in Cisco processes

Cisco has dedicated departments in place to instill and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Cisco Webex environment to our customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Cisco Webex into our customers' hands.

Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to Cisco Webex.

Cisco InfoSec is also responsible for continuous improvement in Cisco Webex's security posture.

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches
- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, PSIRT may alert customers, even without full availability of patches

In all cases, PSIRT discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.

Learn more about PSIRT online at cisco.com/go/psirt.

Security responsibility

Although every person in the Cisco Webex group is responsible for security, following are the main roles:

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications
- Vice president, engineering, Cisco Cloud Collaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

© 2020 Cisco and/or its affiliates. All rights reserved.

Internal and external penetration tests

The Cisco Webex group conducts rigorous penetration testing regularly, using internal assessors. Beyond its own stringent internal procedures, Cisco InfoSec also engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identifying critical application and service vulnerabilities and proposing solutions
- Recommending general areas for architectural improvement
- Identifying coding errors and providing guidance on coding practice improvements

Third-party assessors work directly with the Cisco Webex engineering staff to explain findings and validate the remediation. As needed, Cisco InfoSec can provide a letter of attestation from these vendors.

Cisco Webex Data Center Security

Cisco Webex is a Software-as-a-Service (SaaS) solution delivered through the Cisco Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Cisco Webex Cloud is a communications infrastructure purpose-built for real-time web communications.

Cisco Webex meeting sessions use switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the world. Cisco operates the entire infrastructure within the Cisco Webex Cloud with industry-standard enterprise security.

Additionally, Cisco operates network Point-of-Presence (PoP) locations that facilitate backbone connections, Internet peering, global site backup, and caching technologies to enhance performance and availability for end users.

Physical security

Physical security at the data center includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco data centers, access is controlled through a combination of badge readers and biometric controls. In addition, environmental controls (for example, temperature sensors and fire-suppression systems) and service continuity infrastructure (for example, power backup) help ensure that systems run without interruption.

Within the data centers are also “trust zones,” or segmented access to equipment based on infrastructure sensitivity. For example, databases are “caged”: the network infrastructure has dedicated rooms and racks are locked. Only Cisco security personnel and authorized visitors accompanied by Cisco personnel can enter the data centers.

Cisco’s production network is a highly trusted network: only very few people with high trust levels have access to the network.

Infrastructure and platform security

Platform security encompasses the security of the network, systems, and the overall data center within the Cisco Webex Cloud. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening, security patching, and vulnerability scanning and assessment.

All systems undergo a thorough security review and acceptance validation prior to production deployment. Servers are hardened using the Security Technical Implementation Guidelines (STIGs) published by the National Institute of Standards and Technology (NIST). Firewalls protect the network perimeter and firewalls. Access Control Lists (ACLs) segregate the different security zones. Intrusion Detection Systems (IDSs) are in place, and activities are signed and monitored on a

© 2020 Cisco and/or its affiliates. All rights reserved.

continuous basis. Daily internal and external security scans are conducted of Cisco Webex Cloud. All systems are hardened and patched as part of the regular maintenance. Additionally, vulnerability scanning, and assessments are performed continuously.

Service continuity and disaster recovery are critical components of security planning. The Cisco data centers' global site backups and high-availability design help enables the geographic failover of Cisco Webex services. There is no single point of failure.

Cisco Webex Application Security

Cryptography

Encryption at run time

All communications between Cisco Webex applications and Cisco Webex Cloud occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol with high strength cipher suites.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.[1]

Encrypted media can be transported over UDP, TCP or TLS, User Datagram Protocol (UDP) is the preferred transport protocol for media. Media packets are encrypted using either AES 128 or AES 256 based ciphers. Webex Video devices and 3rd party video devices that support media encryption with SRTP use AES-CM-128-HMAC-SHA1. Webex Applications use AES-256-GCM.[2] The key exchange happens over a TLS-secured channel.

End-to-end encryption

For standard meetings, Webex media servers may need to decrypt media for PSTN, transcoding and recording.

However, for businesses requiring a higher level of security, Cisco Webex also provides end-to-end encryption. With this option, Cisco Webex Cloud does not have access to the encryption keys used by meeting participants and cannot decrypt the media streams.

With End to End Encryption, the meeting encryption key is generated by the meeting host and securely distributed to all other participants in the meeting. To secure the meeting encryption key prior to transmitting it via the Webex cloud to each meeting participant, the key is encrypted by the meeting host.

To achieve this, each participant's Cisco Webex client generates 2048-bit RSA public and private key pair and sends the public key to the host's client. The host's client encrypts the meeting key using the participant's public key and returns the encrypted meeting encryption key back to the participant's client. The client can then decrypt the meeting key using its RSA private key.

All meeting data (voice, video, chat etc.) generated by Cisco Webex clients is encrypted using the shared meeting encryption key. Using Webex End to End Encryption meeting data cannot be deciphered by Cisco Webex service.

This end-to-end encryption option is available for Cisco Webex Meetings and Cisco Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported:

- Personal Room meetings
- Join Before Host
- Video-device enabled meetings
- Cisco Webex Meetings Web App
- Linux clients
- Network-Based Recording (NBR)
- Webex Assistant
- Saving session data transcripts, Meeting Notes
- PSTN Call-in/Call-back[3]

[1] Users connecting to a cloud meeting using a third-party video endpoint may be sending and receiving unencrypted media streams. Configuring your firewall to prevent unencrypted traffic to and from Cisco Webex helps keep your meetings safe. However, allowing attendees outside your firewall to join your meeting using third-party devices can still send your meeting data unencrypted on the Internet.

[2] Support for Webex Applications using AES-256-GCM for media encryption is being rolled out, starting June 2020

[3] When end-to-end encryption is enabled, if the *Pro-E2E-UnencryptedAudio* session type is used, only Webex apps use end-to-end encryption, media from PSTN users is not end-to-end encrypted.

© 2020 Cisco and/or its affiliates. All rights reserved.

Different ciphers

Cisco Webex supports following cipher suites for secured communications. Cisco Webex will allow the strongest possible cipher for the customer's environment. Table 1 outlines cipher suites and each suite's bit length.

Table 1. Cipher suites and bit lengths

Cipher suites	Bit length
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	127

Protecting data at rest

When configured by the customer to do so, Cisco Webex Meetings stores meeting and user data that may be critical to your business. Cisco Webex Meetings uses the following safeguards to protect data at rest:

- Stores all user passwords using SHA-2 (one-way hashing algorithm) and salts
- Encrypts other passwords such as for meetings or recordings
- Encrypts stored Network Based Recordings. Webex recordings are encrypted both at the file level and at the logical volume level. The file key is a 256-bit AES GCM key. This file key is then encrypted with a master key based on AES 256 that is rotated based on policy and saved to a hardware security module (HSM). During the playback and download flow, the encrypted recording file is then decrypted before or during the operation. Cisco maintains these keys for the customer.

Cisco Webex Role-Based access

Cisco Webex application behavior is built from the ground up around five roles, each of which is granted different privileges. They are described below.

Host

The host schedules and starts a Cisco Webex meeting. The host controls the meeting experience for everyone and makes relevant decisions while scheduling the meeting and during it.

The site administrator (a role described later) can mandate many of these controls. If they are not mandated, then the host can make choices on how to secure meetings.

Alternate host

While scheduling, the host can assign alternate hosts, who can start the meeting in lieu of the host and essentially have the same set of privileges as the host.

A host can also pass on his or her privileges to another user during the meeting. With respect to security, there is no difference between the host and alternate host.

© 2020 Cisco and/or its affiliates. All rights reserved.

Presenter

A presenter can share presentations, specific applications, or an entire desktop. The presenter controls the annotation tools. From a security standpoint, the presenter can grant and revoke remote control over the shared applications and desktop to individual attendees.

Panelist (in training and events only)

A panelist is primarily responsible for helping the host and presenter keep the event running smoothly. Any number of attendees can be panelists. The host may ask panelists to serve as subject matter experts, viewing and answering attendee questions in a Q and A session; respond to public and private chat messages; annotate shared content; or manage polls as the polling coordinator.

Attendee

Attendees have no security responsibilities or privileges unless they are assigned the presenter or host role. Ultimately, the site administrator and the host can allow an attendee to grab the Cisco Webex ball (presenter role) anytime in the course of the meeting. This setting is off by default.

Site administrator

This role is authorized for managing accounts as well as for managing and enforcing policies on a site basis or per-user basis. The administrator can choose the Cisco Webex capabilities that are available to all other roles and users.

Administrative capabilities

Cisco Webex has granular site administration capabilities to effectively align your Cisco Webex site with your business needs. This section describes the main security-related features. For further information on all security features, please refer to the Cisco Webex site administration guide here.

Account management

You can integrate your identity management technology with Cisco Webex to allow single sign-on and give you full control over account management and access policies. When your accounts are kept in Cisco Webex, a number of site administration capabilities allow you to manage accounts according to your needs.

- SSO support for SHA-2 SSL certificates

The site administrator can carry out the following actions:

- Lock out an account after a configurable number of failed login attempts
- Automatically unlock a locked-out account after a specified time interval
- Deactivate accounts after a defined period of inactivity Require a user to change the password at the next login Lock or unlock a user account
- Activate or deactivate a user account
- Require security text on new account requests Require email confirmation of new accounts Allow self-registration (sign-up) for new accounts
- Configure rules for self-registration of new accounts
- Set a security option to automatically end a meeting if there is only one participant present

Additionally, the administrator can manage password criteria using the following options:

- Mixed case
- Minimum length
- Minimum number of numeric, alphabetic, or special characters
- No character to be repeated three times or more
- No reuse of a specified number of previous passwords
- No dynamic text (site name, host's name, username)
- No passwords from a configurable list (for example, "password")
- Minimum time interval before password change
- Change of account password by the host at a configurable time interval
- Change of account password by all users at the next login
- Download a site configuration audit log that shows configuration changes made to "Options under Common Site Settings"
- Require authentication to retrieve a host key from a site for scheduled meetings
- Disable the ability for hosts to upload a personal

© 2020 Cisco and/or its affiliates. All rights reserved.

Meeting settings

The granular settings for meetings can be used to manage the behavior of users and system before, during, and after meetings. In most cases these settings can be applied at the center level to allow Cisco Webex Meetings, Cisco Webex Events, and Cisco Webex Training to behave differently and be aligned with required use cases for all users. In addition, many in-meeting features such as file transfer, desktop sharing, and recording can be enabled or disabled for a group of users using customized session types.

Meeting settings can:

- Allow users to store their names and email addresses to easily host and join future meetings
- Allow hosts to reassign recordings to other hosts
- Require authentication for all hosts and attendees to access the site
- Apply strong password rules to remote access service Hide all meetings that are currently publicly listed Mandate a password for all meetings
- Require administrator approval of a "Forgot Password?" request
- Allow hosts to let other hosts schedule on their behalf
- Allow a host to appoint an alternate host when scheduling
- Enable content sharing with external integrations such as Dropbox and Box (when presenting from an iPad)
- Automatically end meetings in a configurable time if there is only one participant left; applies for scheduled meetings, Personal Room meetings, and audio-only meetings
- Enforce a meeting password when joining by phone or video conferencing system
- Enforce a disclaimer to any attendee (including a host) joining a meeting
- Enforce a disclaimer to any attendee prior to viewing or downloading a recording
- Allow attendees to join before the host
- Allow attendees to join telephony before the host
- Restrict the viewing of recordings to signed-in users Prevent the download of recordings
- Enforce passwords for all network-based recordings

For most of these settings the site administrator can choose to leave a setting at a lower security level for the entire site. Hosts can then make security decisions for specific meetings based on need. For example, the site administrator may not require a sign-on to join meetings, but individual hosts can choose to secure specific meetings by allowing only signed-on attendees.

Personal Room security settings

Every Cisco Webex host can be given a dedicated URL for a Personal Room that can be used for meetings. The Personal Room URL is structured as follows: https://sitename.webex.com/meet/username. The host or the Cisco Webex administrator can change the username. Collaboration becomes much easier with Personal Rooms because attendees don't have to look for emails or calendars to join a meeting. The Personal Room can be thought of as a personalized virtual room where a host is available.

When it comes to securing the Personal Room, the Cisco Webex administrator can:

- Require attendees authenticate prior to entering the host's Personal Room (Webex Meeting clients and video endpoints)
- Allow or not allow attendees to notify the host when they are in the lobby (a waiting area)
- Lobby available for Webex Meeting clients and video endpoints
- Enforce the host PIN length (to be used to enter the Personal Room from a video endpoint)
- Enforce unauthenticated attendees to be blocked in lobby even in a room, until admitted by hosts

As a Personal Room host, you can:

- Manually lock your room
- Configure your room to automatically lock after a specified duration (applies to Personal Rooms
- that are started on the Webex Meetings client and
- video endpoints)
- Require that meeting participants who join a Personal Room that is locked be placed in the lobby and the host will have the ability to manually admit them into the meeting
- Place configured authenticated attendees in the lobby, even when your room is open and require you to manually admit them. This is similar to real-world meeting rooms, where authorized employees can just walk into any room, but unauthorized visitors have to be escorted

© 2020 Cisco and/or its affiliates. All rights reserved.

- Enable an email notification to be sent to you in the event someone enters your Personal Room lobby while you are away

Single Sign-On

Cisco Webex supports federated authentication for user Single Sign-On (SSO) using the Security Assertion Markup Language (SAML) 2.0 protocol.

The site administrator will have to upload a public key X.509 certificate to the customized Cisco Webex site.

You can then generate SAML assertions containing user attributes and digitally sign the assertions with the matching private key. Cisco Webex validates the SAML signature against the preloaded public key certificate before authenticating the user.

Those assertions are exchanged between the customer's access management or identity solution and the Cisco Webex site. The customer's solution (for example, Microsoft Active Directory Federation Services, PingFederate, CA Siteminder Single Sign-On, OpenAM, or Oracle Access Manager) acts as an Identity Provider (IdP). The Cisco Webex site acts as the service provider. Cisco Webex supports both service-provider-initiated and IdP-initiated SSO flows.

Implementing single sign-on on Cisco Webex gives you complete control over user and access management to meet your corporate policies. Some benefits:

- The IdP is the authority for validating user credentials (which can be a certificate, fingerprint, or other)
- Customers can implement two-factor authentication for users centrally rather than have each SaaS-based service use a different solution
- Cisco Webex does not store any user credentials Customers control who accesses Cisco Webex
- Onboarding and off-boarding users as they join or leave the corporate IdP is transparent

Additional Cisco Webex features and security

Join meetings with video devices

Users can join or start a Cisco Webex Meeting with a video device. This capability can be optionally made available on a Cisco Webex Meetings site. Once turned on, a user can use a Cisco TelePresence® endpoint, a soft client, a Skype for Business client, or any third-party standards-based video device to join meetings by dialing the meeting video address. Experience is amazing with Cisco end points as a user can join a meeting on a device by automatic wireless pairing.

There is no additional video bridging equipment is required on the customer premises for video devices to work. The video-bridging capabilities are deployed in the same highly secure Cisco Webex Cloud as the Cisco Webex Meeting Center and use the same industry-grade security controls (physical, network, infrastructure, and administrative). Video endpoints can join meetings over Session Initiation Protocol (SIP) and H.323 for signaling and Real-Time Transport Protocol/Secure Real-Time Protocol (RTP/SRTP) media. Webex Meetings supports TLS transport for SIP and SRTP for media. When video endpoints join a meeting over SIP/TLS, the media stream is encrypted through SRTP.

H.235 is used to secure H.323 connections.

Additionally, a site can be configured to require passcodes for joining meetings using a video device.

Cloud Connected Audio

Cisco Webex Cloud Connected Audio (CCA) is an end-to-end audio solution that uses your on-premises IP telephony network to provide an integrated audio experience for your Cisco Webex meetings. Cisco Webex CCA implements a Session Initiation Protocol (SIP) trunk from your premises into the Cisco Webex data center instead of using a traditional telephony connection. This solution provides the same integrated and intuitive user experience as all other Cisco Webex audio options. However, by directly using your IP telephony network, Cisco Webex CCA can provide more attractive audio pricing.

CCA is a fully encapsulated environment. Reaching it from the Internet or perpetrating any kind of an attack is extremely difficult. Although the infrastructure is shared, there is no inter-tenant routing, so malicious traffic from other tenants is blocked. Furthermore, traffic over the trunk is limited to routing protocols and User Datagram Protocol (UDP) packets to desired Cisco Webex infrastructure ports. The Cisco Webex infrastructure is configured to receive traffic from preconfigured dial peers only.

© 2020 Cisco and/or its affiliates. All rights reserved.

CCA connectivity is established through point-to- point private connections to the Cisco Webex platform. CCA circuits are terminated on dedicated customer ports.

Access control lists on edge routers and firewalls in both the customer's and Cisco's data centers secure the circuits.

CCA Service has segmented IP subnets, and only the Cisco Webex Cisco Unified Border Element (CUBE) IP segment is advertised to customers. No customer has any visibility into another customer's IP or CUBE.

To conclude, Cisco Webex CCA offers strong security without introducing unnecessary overhead to the traffic or encumbering the design.

Cisco Webex privacy

Customer data protection, retention, and compliance
Cisco Webex takes customer data protection seriously. We collect, use, and process customer information only in accordance with the Cisco Privacy Statement. The Cisco Webex Terms of Service provides additional information.

Cisco Webex Meetings is Privacy Shield Framework-certified.

Cisco Webex will, pursuant to appropriate lawful transfer mechanisms, transfer the administrative data, support data, and telemetry data from the EU to United States (and where appropriate, to other permissible locations). The definitions of these categories of data are provided below.

Administrative data: Information about employees or representatives of a customer or other third party that is collected and used by Cisco in order to administer or manage Cisco's delivery of products or services, or to administer or manage the customer's or third party's account for Cisco's own business purposes. Administrative data may include the name, address, phone number, email address, and information about the contractual commitments between Cisco and a third party, whether collected at the time of the initial registration or later in connection with the management or administration of Cisco's products or services.

Administrative data may also include the meeting title, time, and other attributes of the meetings conducted on Cisco Webex by employees or representatives of a customer. Other examples of administrative data may include meeting title, meeting time, and other attributes of the meetings hosted on Cisco Webex.

Customer data: All data (including text, audio, video, image files, and recordings) that is either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, or developed by Cisco at the specific request of a customer pursuant to a statement of work or contract. Customer data includes log, configuration, or firmware files, and core dumps. It is data taken from a product or service and provided to Cisco to help us troubleshoot an issue in connection with a support request. Customer data does not include administrative data, support data, or telemetry data.

Support data: Information that Cisco collects when a customer submits a request for support services or other troubleshooting, including information about hardware or software. It includes details related to the support incident, such as authentication information, information about the condition of the product, system, and registry data about software installations and hardware configurations, and error-tracking files. Support data does not include log, configuration, or firmware files, or core dumps taken from a product and provided to us to help us troubleshoot an issue in connection with a support request, all of which are examples of customer data.

Telemetry data: Information generated by instrumentation and logging systems created through the use and operation of the product or service.

All data collected in Cisco Webex Cloud is protected by several layers of robust security technologies and processes. Below are examples of controls placed in different layers of Cisco Webex operations to protect customer data:

- **Physical access control:** Physical access is controlled through biometrics, badges, and video surveillance.
  Access to the data center requires approvals and is managed through an electronic ticketing system.
- **Network access control:** The Cisco Webex network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco Webex data center is continuously monitored using an Intrusion Detection System (IDS). The Cisco Webex network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and Access Control Lists (ACLs).

© 2020 Cisco and/or its affiliates. All rights reserved.

- **Infrastructure monitoring and management controls:** Every component of infrastructure, including network devices, application servers, and databases, is hardened to stringent guidelines. They are also subject to regular scans to identify and address any security concerns.
- **Cryptographic controls:** As noted earlier, all data to and from the Cisco Webex data center to Cisco Webex clients is encrypted, except for unencrypted video devices in a cloud-enabled meeting. Additionally, critical data stored in Cisco Webex, such as passwords, is encrypted.

Cisco employees do not access customer data unless access is requested by the customer for support reasons. Access to systems in this case is allowed by the manager only in accordance with the "segregation of duties" principle. It is granted only on a need-to-know basis and with only the level of access required to do the job. Employee access to these systems is also regularly reviewed for compliance. Employees with such access are required to take annual International Organization for Standardization (ISO) 27001 Information Security Awareness training.

In addition to these specialized controls, every Cisco employee undergoes a background check, signs a Nondisclosure Agreement (NDA), and completes Code of Business Ethics (COBE) training.

Health Insurance Portability and Accountability Act (HIPAA)

Cisco can provide information regarding the functionality, technology, and security of Cisco Webex. A HIPAA-covered entity would need to consult with its own legal counsel to determine whether Cisco Webex's functionality is compliant for its business processes and GDPR ready.

- GDPR readiness
- Cisco Webex Meetings privacy sheet

Industry standards and certifications

In addition to complying with our stringent internal standards, Cisco Webex also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Webex is:

- ISO 27001 certified
- Service Organization Controls (SOC) 2 Type II audited
- FedRAMP certified (visit cisco.com/go/fedramp for more details, scope, and availability)
  Note: FedRAMP certified Webex service is only available to U.S government and education customers
- Cloud Computing Compliance Controls Catalogue
- (C5) attestation
- Privacy Shield Framework certified

Conclusion

Be collaborative and get more done, faster, using Cisco Webex solutions, a proven industry leader in web and video conferencing. Cisco Webex offers a scalable architecture, consistent availability, and multilayer security that is validated and continuously monitored to comply with stringent internal and third-party industry standards. We connect everything more securely to make anything possible.

How to buy

To view buying options and speak with a Cisco sales representative, visit www.cisco.com/c/en/us/buy.

For more information

To learn more about Cisco Webex solutions, visit our site:

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support
- Cisco Webex Cloud Connected Audio

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

FAQ: International Transfer of Personal Data post-Schrems II

At Cisco, fostering relationships with our Customers and Partners based on trust is of utmost importance. We believe that privacy is a fundamental right and our Customers' and Partners' privacy and security are always Cisco's top priority.

We understand that the Schrems II judgment of the Court of Justice of the European Union (CJEU) (and the consequent decision of the Switzerland's Federal Data Protection and Information Commissioner) might be difficult to navigate for our Customers and Partners. As the European Commission and the US Department of Commerce work through the decision and develop a path forward, we would like to reassure you that we have taken steps to enable the seamless, legal cross-border transfer of personal data in accordance with EU and Swiss privacy requirements.

1. What is "Schrems II"?

Schrems II is a case before the CJEU brought by the Irish High Court challenging the validity of the Standard Contractual Clauses (SCCs) to provide adequate safeguards in accordance with EU standards.

In its judgment, the CJEU decided on 16 July 2020 that the EU-US Privacy Shield could no longer be used as a valid personal data transfer mechanism due to concerns over US surveillance law. In the same ruling, the CJEU reaffirmed the validity of the SCCs as a transfer mechanism, subject to certain conditions. Data exporters (i.e. companies transferring personal data outside of the EU – e.g. Cisco EU Customers), where appropriate with the collaboration of the data importer (e.g. Cisco), will now have the responsibility to verify on a case by case basis if the law of the third country provides adequate protection of data transferred under EU data protection law, taking into account the circumstances of transfer and possible additional safeguards, if required.

Further guidance from the European Data Protection Board (EDPB) following the Schrems II decision interprets the ruling as applying in the context of BCRs, meaning the circumstances of transfer should also be assessed. The court's ruling took effect immediately, and the US Department of Commerce and European Commission are currently working on a path forward.

©2020 Cisco and/or its affiliates. All rights reserved

2. Why is Cisco still certified under the Privacy Shield Frameworks and why are they still mentioned in the Cisco Online Privacy Statement?

Cisco is certified under both the EU-US and Swiss-US Privacy Shield Frameworks, which were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union or Switzerland to the United States.

The US Department of Commerce, issued guidance stating The decisions of the CJEU and the consequent opinion of Switzerland's Federal Data Protection and Information Commissioner (FDPIC) do not relieve participants in the EU-US and Swiss-US Privacy Shields of their obligations under the Privacy Shield Frameworks as the US Department of Commerce continues to administer the Privacy Shield program (including processing submissions for re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List). As such, Cisco continues to meet these obligations regardless of whether the mechanisms are still used to transfer data of EU or Swiss customers.

3. What are the SCCs and does Cisco use them?

The European Commission's Standard Contractual Clauses (SCCs) are contractual terms that have been pre-approved by the European Commission and serve as a legal basis for personal data transfers outside the EU/EEA. SCCs have been available to companies for over 10 years to provide safeguards according to European standards to personal data outside of the EU/EEA and we have been using them as a data transfer mechanism for several years. They have always been an integral part of our Master Data Protection Agreement (MDPA), which is required for Cisco suppliers and available to customers, to enable safe and legal transfers of personal data outside of the EU. Cisco has also executed an inter company personal data transfer agreement incorporating the SCCs. This agreement obligates Cisco entities outside of the EU/EEA, receiving personal data from Cisco entities located inside the EU/EEA, to process such personal data in accordance with the terms of the SCCs.

4. What are Cisco's Binding Corporate Rules?

Binding corporate rules (BCRs) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They are legally binding and enforced by every member concerned within the group. BCRs require approval by the competent data protection authority in the EU.

Our Binding Corporate Rules – Controller (BCR-C) have been approved by the European data protection supervisory authorities. This approval demonstrates that Cisco's Data Protection & Privacy Program is aligned with EU requirements, including the GDPR. Cisco's BCR-C set forth the mandatory, minimum standards for handling EU personal data by Cisco, as a data controller (e.g. customer relationship management). Our approved BCR-C serve as a legally valid transfer mechanism and commits Cisco to processing EU personal data in accordance with EU data protection standards anywhere that Cisco operates in the world.

©2020 Cisco and/or its affiliates. All rights reserved

In addition to this, we are delighted to let you know that our Binding Corporate Rules – Processor (BCR-P) have been submitted for approval to the competent data protection authority in the EU. Like Cisco's BCR-C, the BCR-P sets forth the mandatory and minimum standards for handling EU personal data by Cisco, when Cisco acts as a data processor (e.g. when we provide services on behalf of our customers) and will also serve as an additional legally valid transfer mechanism in this respect.

5. Does Schrems II affect Cisco's transfer of personal data to the US and other countries?

We would like to reassure you that we can transfer personal data to the US and other countries on the basis of the SCCs when we act as a processor (i.e., when we provide services on behalf of our customers) and on the basis of our BCR-C when acting as controllers (e.g., human resources data, administrative data, billing information, customer relationship management, etc.).

We will also be able to use our BCR-P, once approved, as a valid transfer mechanism when we act as processors. Furthermore, when the new module of the EU Code of Conduct for the transfer of personal data will be completed and approved, Cisco will also be able to use this as an additional valid transfer mechanism when acting as a processor in the context of Cloud Services.

6. How does the Schrems II decision impact Cisco's Customers and Partners?

The vast majority of Customers and Partners have concluded SCCs with Cisco. . Therefore, while Customers and Partners should assess the law of countries to which data is transferred, the circumstances of transfer and the additional safeguards put in place by Cisco as outlined below, for those who have concluded SCCs there is no need to change terms of the contract.

If you are unsure about whether you have concluded a MDPA with us, please reach out to your Cisco representative.

7. Where is my data located?

We encourage you to consult our Privacy Data Sheets and Data Maps, which illustrate on a per-offer basis what personal data we process, how we process it and where the data is located (including our European Data Centers). They also outline what additional security measures we have put in place for specific offers that potentially handle more sensitive information (e.g. end-to-end encryption for communication with Webex Meetings).

8. What is meant by FISA 702 and EO 12333? How do they relate to Schrems II?

Section 702 of the Foreign Intelligence Surveillance Act (FISA 702) is a US statute establishing a judicial process authorizing a specific type of data acquisition. Under FISA 702, an independent court may authorize the US government to issue orders requiring US companies to disclose communications data of specific non-US persons located outside of the US to obtain specific types of foreign intelligence information.

©2020 Cisco and/or its affiliates. All rights reserved

Executive Order 12333 (EO 12333) is a general directive organizing US intelligence activities. Unlike FISA 702, EO 12333 does not authorize the US government to require any company to disclose data, though it may be used to authorize clandestine intelligence activities involving overseas access to data without the involvement of the company in question.

In its decision, the CJEU ruled that where transfers of personal data to the US are subject to FISA 702 and EO 12333 the transfer mechanism used does not provide an essentially equivalent protection as EU law.

9. Are the transfers of personal data by Cisco subject to FISA 702 or EO 12333?

Webex Teams, Meetings, Meraki and other Cisco SaaS offers are considered electronic communication services or remote computing services. Therefore,transferred customer data in that context may theoretically be within the scope of FISA 702. It is very important to note, however, that communications data (usually targeted by FISA 702) for Webex Teams, Meetings and Meraki are generally stored in the customer's region and not subject to transfer to the US. Moreover, the numbers of US National Security Demands, including FISA Orders, are included in our transparency report on government demands for data, which we publish twice a year. We are not directly subject to surveillance requirements under EO 12333 nor voluntarily cooperating with any program authorized by the EO. In accordance with the ruling of the Schrems II decision, supplementary measures should be put in place when data is transferred to third countries where essentially equivalent protection is not legally available in order to ensure appropriate safeguards are in place. Please refer to the next answer for details on the additional safeguards being taken by Cisco.

10. Does Cisco provide additional safeguards for transfers to the US that are potentially subject to FISA 702 Orders or EO 12333 authorised programs?

We are currently awaiting guidance from the EDPB on what kind of legal, organisational and technical supplementary measures could be provided post-Schrems II. In the meantime, on top of our holistic approach to privacy and security, we can demonstrate measures we are already taking that limit disproportionate access by government authorities to our Customers' and Partners' data.

Legal measures

On top of complying with the SCCs, we commit to a principle-based review to examine government demands for data and appropriately narrow and challenge requests which are not necessary and proportionate. We will notify our customer (unless such notification is prohibited by law) to give them the opportunity to limit or prevent disclosure. We also challenge requests that prohibit notification to the customer. Please be aware that we will only provide the data to an agency with appropriate authority under applicable law to demand this data from us and we will only provide the specifically requested information or data in certain limited circumstances.

Transparency measures

We publish a Transparency report detailing numbers of government demands detailing numbers of accepted and rejected government demands for data twice a year. This gives every customer the opportunity to see for themselves how many inquiries are received and that no EU personal data has been handed over to authorities in the USA so far.

©2020 Cisco and/or its affiliates. All rights reserved

We also make use of verifications mechanisms such as privacy and data security certifications (including but not limited to ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II and SOC 3). These demonstrate data minimization and organizational security measures that limit the pool of data available for access and protect against unauthorized access.

Technical and organizational measures

In addition to this, our Privacy Data Sheets and Data Privacy Maps outline how, where and by whom personal data is processed across our portfolio of solutions. Our Privacy Data Sheets provide also details on our offer-specific security and organisational measures, including where we encrypt data during transit (safeguarding against access under EO 12333 during transfers to the US) and at rest.

A key priority for Cisco is the secure processing of personal data through appropriate technical and organizational measures. Only a technically secure environment ensures confidentiality, integrity and availability. Cisco ensures uniform implementation throughout the company with appropriate data protection and data security policies (e.g.: Security Vulnerability Policy, BCRs etc.), with an industry-leading security design and leading-edge encryption. Cisco Webex Meetings customers, for example, can opt for true end-to-end encryption (E2EE) of video, audio, text, and meeting content. With E2EE enabled by the administrator, Cisco Webex does not have access to the encryption keys used by meeting hosts and participants and cannot decrypt the data nor media streams. With E2EE, the meeting encryption key is generated by the meeting host and securely distributed to only the meeting participants. This makes interception and reading impossible, also by Cisco itself.

Moreover, Cisco regularly undergoes independent testing and certification. Cisco's IT security certifications include ISO 27001, ISO 27017, ISO 27018, SOC 2 and SOC 3, as well as BSI C5 (Cloud Computing Compliance Controls Catalog). Last but not least, through research and development, Cisco ensures that the technical measures are constantly improved to the highest level (e.g. post-quantum encryption).

11. Are these safeguards applicable to transfers to other countries than the US?

The Court's ruling upholds the validity of transfers using SCCs to third countries in general, not just to the US. While the Court did not reach conclusions on the essential equivalence of any other third country laws, the same assessments and thresholds for transfer will also apply.

While most transfers of personal data out of the EEA will be to the US, some Cisco services, such as Technical Assistance (TAC) Service Delivery, may involve transfers to other third countries. As such, please be assured that the legal, technical and organizational safeguards as well as transparency measures mentioned above are globally applicable

12. How will Brexit affect data flows to and from the UK?

The Withdrawal Agreement agreed between the UK and the EU allows for a transition period until the end of 2020. There is no change regarding data flows to and from the UK during this transition period. As of 1st January 2021, the UK will be deemed a third country. The UK government is seeking an adequacy finding from the EU during the transition period.

©2020 Cisco and/or its affiliates. All rights reserved

If the UK and EU do not come to an agreement on data protection during the transition period, the UK will become a third country in the eyes of the EU Commission. In that case, lawful transfer of personal data from the EU to the UK will have to be subject to an approved transfer mechanism that provides appropriate safeguards. The UK government and the UK data protection authority (ICO) have stated they will recognize all 27 EU member states as providing adequate protection for personal data of UK individuals. Therefore, the transfer of personal data of UK individuals to EU member states will be unaffected until the UK Government states otherwise.

If there is no agreement on data protection by the end of the transition period Cisco will enter into the SCCs with EU based customers where the service involves a transfer of their personal data to the UK. This means EU based customers can continue to use a Cisco service where personal data is processed in the UK.

13. Where do I get more general information on the processing and transfer of Personal Data by Cisco?

We invite you to consult our Trust Center for all our efforts to keep customer data, including personal data secured with privacy properly respected and for all updates in this regard. For specific information, we invite you to contact your Cisco representative.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Cisco Technical Assistance (TAC) Service Delivery

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco TAC.

1. Overview Cisco TAC Delivery Capabilities

Cisco's Support Services Technical Assistance Center (TAC) is a global organization that provides around-the-clock, award-winning technical support services online and over the phone. TAC offers customer support for all Cisco products/services using a global follow-the-sun support model. Our TAC teams support thousands of service requests every day, as well as supply best-in-class hardware support, repair, and replacement from one of our 1,100 depots.

As part of our TAC services support process, service requesters may be required to provide certain personal data. These data are limited to business contact details provided by the requester and used for the purposes of providing the support required.

Customer Case Attachment Data (including text, audio, video or image files), which are either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, or data developed by Cisco at the specific request of a customer, is subject to the following security controls:

- Authentication
- Access control
- Login/activity logging and monitoring
- Data masking
- Data encryption, both at rest and in transit
- Transport and storage for physical data

2. Personal Data Processing

The tables below list the personal data used by Cisco TAC to carry out the services and describe why we process that data.

©2020 Cisco and/or its affiliates. All rights reserved.

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Information About the Condition of the System • Registry Data About Software Installations and Hardware Configurations • Error-Tracking File	We use TAC Support Information to: • Provide remote access support • Review quality of the support service • Perform analysis of the service solution
Customer Case Attachment	Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. We instruct customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be processed for Customer Case Attachments for the purpose of providing support: • Device Configuration (e.g., running config and startup config, SNMP Strings (masked); Interface description • Command Line Interface (CLI) (i.e., Show Commands, such as Show Version) • Product Identification Numbers • Serial Numbers • Host Names • Sysdescription (has device location) • IP Addresses • Operating System (OS) Feature Sets • OS Software Versions • Hardware Versions • Installed Memory • Installed Flash • Boot Versions • Chassis Series • Slot IDs • Card Types • Card Families • Firmware Versions • MAC Address • SNMP MIBs (ACLs, CDP)	We use Customer Case Attachments to: • Provide remote access support • Perform analysis of the service solution

©2020 Cisco and/or its affiliates. All rights reserved.

3. Cross-Border Transfers

Cisco TAC leverages a Customer Relationship Management (CRM) case management system to deliver our services and capture TAC Support Information. This system is a customized instance on the SalesForce.com (SFDC) platform known as Support Case Manager (SCM) and utilizes a numerical Service Request (SR) case assignment process. Cisco TAC SR case details and associated case notes within Cisco's CRM system are stored at the Salesforce.com (SFDC) data center, which physically resides in Washington DC, USA.

Customer Case Attachments (including detailed system logs, etc.) uploaded by customers are housed in a single data repository hosted by Amazon Web Services (AWS -US East, North Virginia Region). The AWS instance, known internally as CX Files, maintains robust data security and governance controls, including authentication, authorization, role-based access controls, encryption in transit and at rest, login logging and monitoring, and activity logging and monitoring. CX Files is wholly maintained by the Cisco Customer Care IT / Crypto team and the storage location is not shared with any other AWS customers, nor with any other team within Cisco.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Cisco TAC Support Information	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.
Customer Case Attachments*	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.

**As stated above, Customer Case Attachment Data (including text, audio, video or image files), which are either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, and/or data developed by Cisco at the specific request of a customer, are subject to the above-mentioned security controls.*

5. Data Portability

©2020 Cisco and/or its affiliates. All rights reserved.

Cisco TAC allows customers to export both their Service Request (SR) case data and Case Attachments related to cases for which they have been granted access. Partners who have been enabled by the customer and assigned to a specific contract, may also view, upload and/or download data on the customer's behalf.

6. Data Deletion & Retention

Cisco TAC Service Request (SR) case data that has been in CLOSED status for 10 years + 1 day or more is automatically purged from our key repositories on a nightly basis. Case data is all data captured as part of the service request process, including all Case Notes and Customer Case Attachments.

Customers may request deletion of personal data retained by Cisco TAC by submitting a request via privacy portal. If you require deletion of any other data outside of the timelines stated above, please contact your sales representative. In each instance, Cisco will endeavor to delete the requested data from its systems at the earliest possible time and will do so unless the data is required to be retained by Cisco.

Cisco retains data to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customers (i.e., legitimate business purposes).

7. Personal Data Security

Cisco Services has received ISO 27001:2013 (Information Security) re-certification from TUV (a copy of the new certificate is available here).

Personal Data processed by	Type of Encryption
TAC Support Information	Encrypted in transit, and at rest after reaching Cisco.
Customer Case Attachments	Encrypted in transit, and at rest after reaching Cisco.

8. Third Party Service Providers (Sub-processors)

Cisco engages sub-processors that provide the same level of data protection and information security that you can expect from Cisco. A current list of contracted sub-processors for the Cisco TAC Delivery service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Aricent (India) **Estarta (Jordan)** **IBM (Bulgaria)** **Sykes (Costa Rica and Colombia)** **Concentrix (USA)**	TAC Support Information Customer Case Attachments	Delivery support on behalf of Cisco Systems, Inc.	• Gurgaon, India • Amman, Jordan • Sofia, Bulgaria • San Jose, Costa Rica and Barranquilla, Columbia • California, USA
Salesforce.com (USA)	Customer Relationship Management (CRM)	Hosting/Storage	• Washington, DC, USA
Amazon Web Services (USA)	Customer Case Attachments	Hosting/Storage	• US East, Northern Virginia

©2020 Cisco and/or its affiliates. All rights reserved.

9. 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.

10. Certifications and 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. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation (GDPR) and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Customer Experience (CX) has received the following certifications:

- ISO 27001

11. General Information and GDPR FAQ

©2020 Cisco and/or its affiliates. All rights reserved.

For more general information related to Cisco's Technical Services, please visit the Technical Services section Cisco.com.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

©2020 Cisco and/or its affiliates. All rights reserved.