



Possibilities

#CiscoLive

Webex Meetings Security

Tony Mulchrone
Technical Marketing Engineer
Cisco Collaboration Technology Group

DGTL-BRKC0L-2622



June 2-3, 2020 | ciscolive.com/us

#CiscoLive



Agenda

- Cisco's Security and Privacy principles
- Webex Product Overview
- Cisco's Secure Cloud Architecture for Webex Meetings
- Onboarding Users, Authenticating Users, Webex Meetings Apps and Devices
- User Authentication and Authorization, OAuth Tokens
- Secure signalling (TLS), Service and Certificate Validation
- Standard Encrypted Meetings and Meetings with Strong End to End Encryption
- Webex Network Based Recordings and Webex Assistant transcription services
- Webex Meetings App Security - Securing Content, Proximity, Secure Cognitive Collab
- Webex Meetings : Administrative Security Features and Best Practices

“Privacy is a fundamental human right, and we need security and transparency to protect it.”



Chuck Robbins
Chairman and CEO, Cisco
February 7, 2019

Cisco's Security Principals:

Privacy

Committed to the privacy of your data

Security

Secure by design and by default

Transparency

Transparent about security

Privacy & Security at Cisco

Cisco's Security and Trust Organization



Data Protection
Program



Privacy by Default :
Cisco's Secure
Development Lifecycle



Independent
Compliance
Reviews

More information:

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-security-and-trust.pdf

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/data-protection-program-solution.pdf

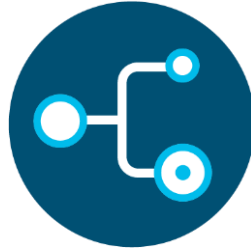
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

<https://www.cisco.com/c/en/us/about/trust-center/webex.html>

Cisco's Data Protection Program



Policies and
Standards



Identification and
Classification



Data Risk
Assessments



Incident
Response



Oversight and
Enforcement



Awareness and
Education



Security & Privacy
By Design

Cisco's Secure Development Lifecycle

Product Security Baselines

200+ Specific security requirements

Vulnerability Testing

Regular automated testing

Whitehat Hacking

Threat Modelling

Education and training

10+ years Cisco SecCon conference

Mandatory employee security training

Cloud Approval To Operate (CATO)

STO Security assessment process

CISCO *Live!*



Independently Audited Compliance Certifications



Cisco Webex Certifications



ISO 27001
ISO 27017
ISO 27018
SOC2 type II
SOC3
FedRAMP Moderate
C5 (Germany)

Regulatory Compliance



GDPR
HIPAA
EU Binding Corp. Rules
EU/US Privacy Shield
Swiss/US Privacy Shield
APEC Cross Border Privacy
Rules

For more information: <https://www.cisco.com/c/en/us/about/trust-center/webex.html>

Webex Meetings Privacy Data Sheet

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 purchase 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 any mobile device or video system as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding the People Insights feature for Cisco Webex Meetings, please see Addendum One below. For a detailed overview of the Service, please visit the Cisco Web Conferencing [homepage](#).

Because the Service enables collaboration among its users, you may be asked to provide your personal data 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. If you choose to purchase the Service, you will need to disclose personal data to Cisco in order to use it. Cisco will use your personal data consistent with this Privacy Data Sheet. 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 as personal as a face-to-face meeting. The meeting host has the option to record meetings and all users have the option to upload and preserve files shared during and outside of meetings, which may be discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording if the meeting host intends to record the meeting. If the meeting host opts not to preserve the meeting content, it disappears from the Webex Meetings platform immediately after the meeting concludes. If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy Data Sheet is accessible by 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. 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 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 lists the categories of personal data used by the Service and describe why we process such data.

Key Information in the Webex Meetings Privacy Datasheet

The types personal data Webex Meetings processes and the purpose of data processing

Details of Webex data center locations and legal mechanisms for data transfer across international boundaries

Who has access to personal data and why

Data Retention and Deletion rules

Securing Personal Data : Data in Transit and Data at Rest, End to End Encryption

Details of Third Party Service Providers

Incident Management (PSIRT)

Certifications and Compliance

Cisco's Master Data Protection Agreement (MDPA)



MASTER DATA PROTECTION AGREEMENT

This MASTER DATA PROTECTION AGREEMENT ("MDPA") is entered into by and between Cisco Systems, Inc. whose registered office is at 170 West Tasman Drive, San Jose, California 95134 and its Affiliates and Cisco International Limited, registered in England and Wales (Company Number 06640658) with its principal place of business at 9-11 New Square Park, Bedford Lakes, Feltham, England TW14 8HA, United Kingdom (collectively "Cisco"), and [please complete] having its principal place of business at [please complete] and its Affiliates ("Customer"), (together "Parties").

This MDPA is governed by the terms of the applicable agreement entered into by and between the Parties for the supply of Products and/or Services by Cisco to Customer ("the Agreement"). In the event of a conflict between this MDPA, including any attachments herein, and the Agreement, the provisions of this MDPA will control but only with respect to the subject matter hereof.

In consideration of the mutual promises and covenants hereinafter contained and of other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1.0 SCOPE OF AGREEMENT. This MDPA is comprised of these General Terms and the following Attachments A-E attached herein, which are incorporated by reference:

1. Attachment A INFORMATION SECURITY EXHIBIT
2. Attachment B DATA PROTECTION EXHIBIT
3. Attachment C *Reserved*
4. Attachment D STANDARD CONTRACTUAL CLAUSES
5. Attachment E GLOSSARY

GENERAL TERMS

2.0 LIMITATION AND EXCLUSION OF LIABILITY.

- 2.1 Nothing in this MDPA limits or excludes the liability of either Party to the other for: (i) bodily injury or death resulting directly from the negligence of the other Party; (ii) fraud or fraudulent misrepresentation; or (iii) any liability that cannot be limited or excluded under mandatory applicable law.

The MDPA describes what Cisco does in terms of :

General Security Practices

General Security Compliance

Technical & Organizational Security Measures

Physical and Environmental Security

Communications Security and Data Transfer

System Development and Maintenance

Penetration Testing and Vulnerability Reports

Data Protection and Privacy

Processing of Personal Data

<https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf>

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-summary-mdpa.pdf

Webex Meetings Product Overview

Webex Meetings Product Overview

Cisco Webex Meetings is a cloud-based service that provides virtual meeting rooms in which participants from diverse locations can collaborate in real time. The core of the Cisco Webex Meetings service offering is hosted conferencing with web, audio video services.

Services Include :

Cisco Webex Meetings – Web and Video Conferencing for up to 1000 participants

Cisco Webex Events - Larger scale Web and Video Conferencing for up to 3000 participants with chat, polling and Q&A

Cisco Webex Training - Online Training with live instruction for up to 1000 participants

Cisco Webex Support - IT support and customer service for your employees and customers

Service Access : - **Webex Desktop/Mobile/Web Apps, IP Voice & Video Devices, PSTN**

User generated meeting content (including chat) is not persisted in the cloud, unless you record

You can choose to store and manage meeting recordings, transcripts and file uploads

Cisco does store user data, billing and analytics data (see [Privacy data sheet](#) for details)

Webex Meetings Cloud Architectural Overview

- Data Centres
- Meetings services
- Cloud Security

Webex Meetings Data Centre Locations

Regional Data Centre Locations



- **Webex Meeting related Services**
- Meetings/ Events/ Training /Support
- Identity
- Site Administration/ Analytics/ Billing
- Recording/ Transcription

• Globally distributed Data Centres

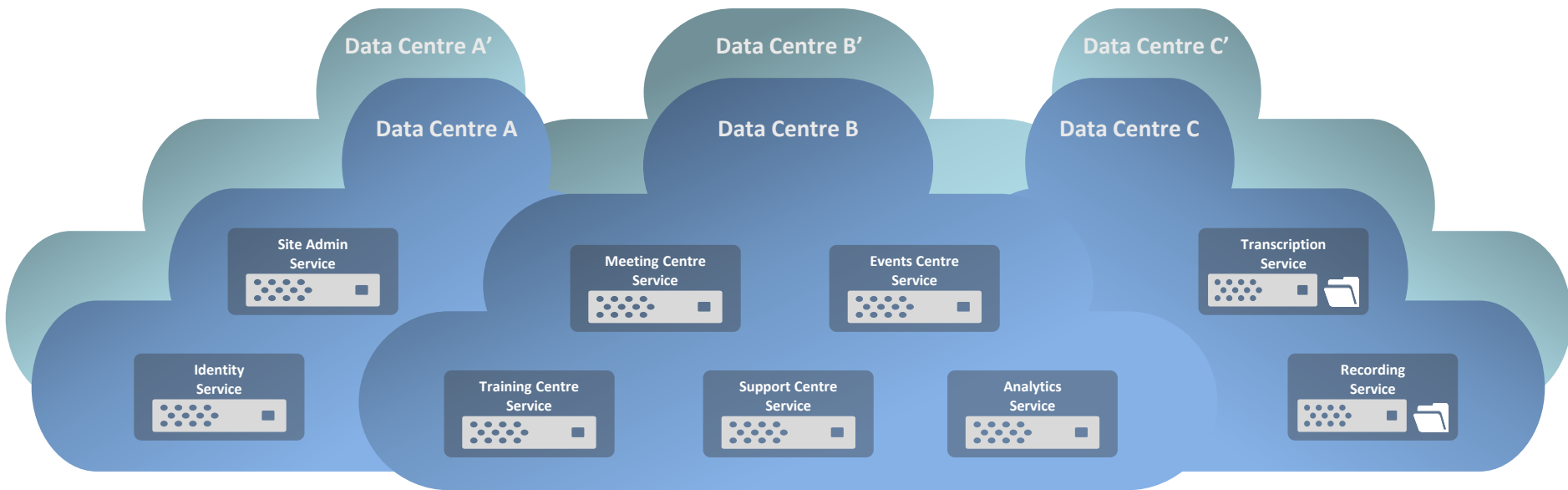
• **Webex Media Services**

- Media Nodes for Webex Meetings and Webex Teams :
- Voice, Video and Content Sharing services
- PSTN access for Meetings
- **Multiple data centre locations worldwide**

 **Webex Meetings-related services (not media)**

 **Webex Media services**

Webex Meetings related Services (not media services)

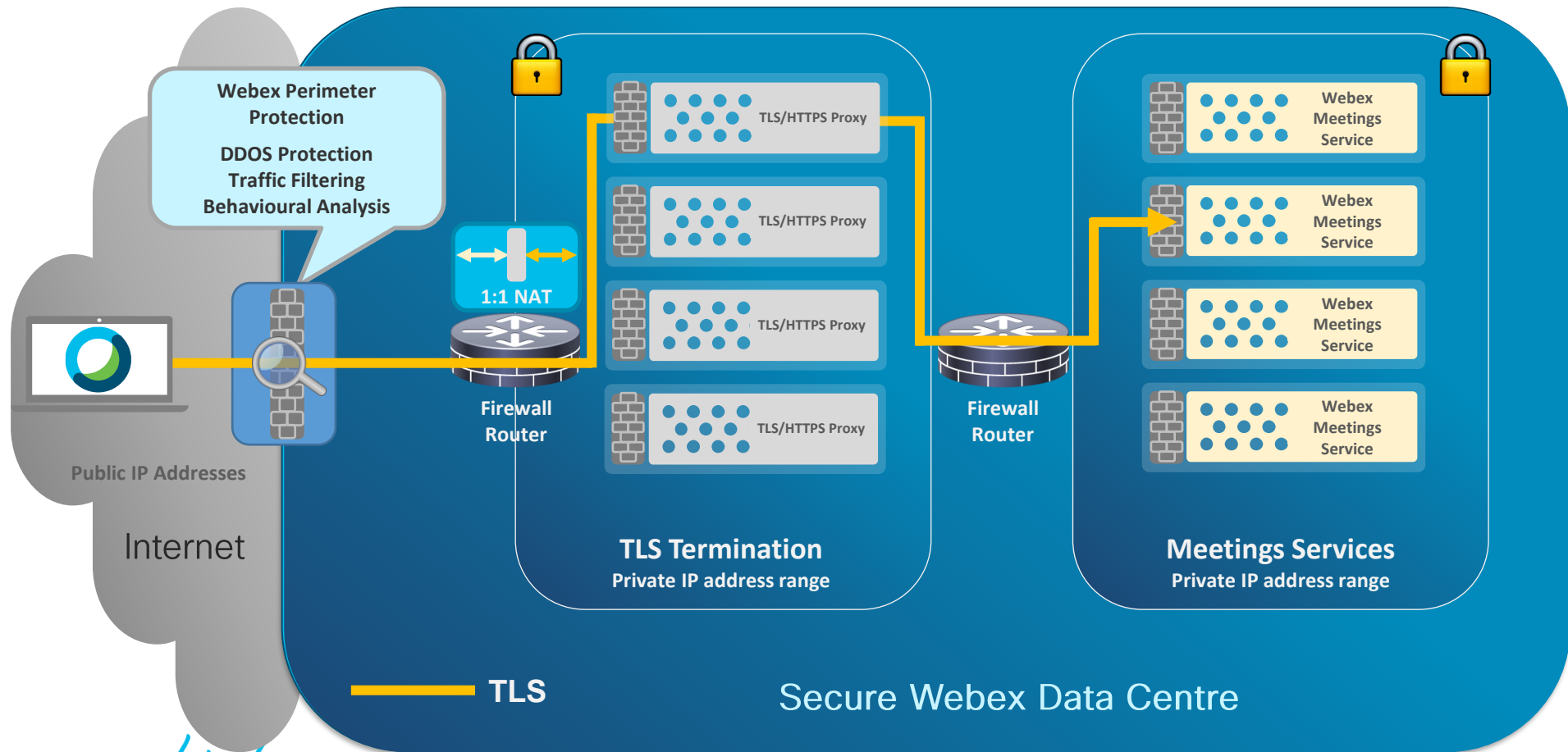


Webex Services for Webex Meetings/Events/Training/Support, Identity, Recording, Transcription, Billing, Analytics and Administration are distributed and replicated across multiple independent data centres.

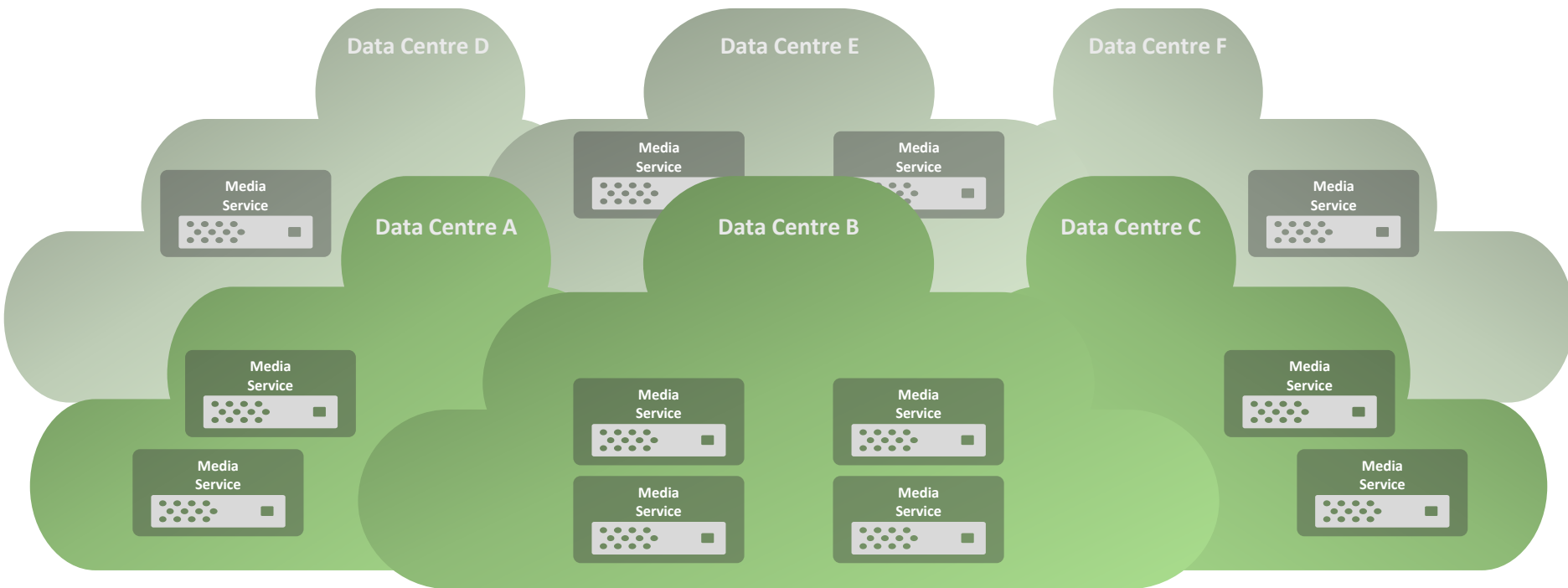
User Generated Content (e.g. Recordings, Transcripts, Uploaded Files) is stored in the data center closest to a Customer's location as provided during the ordering process

Webex Meetings Data residency locations : EMEAR/ APJ/ US/ Australia

Webex Meetings App – TLS/HTTPS signaling traffic

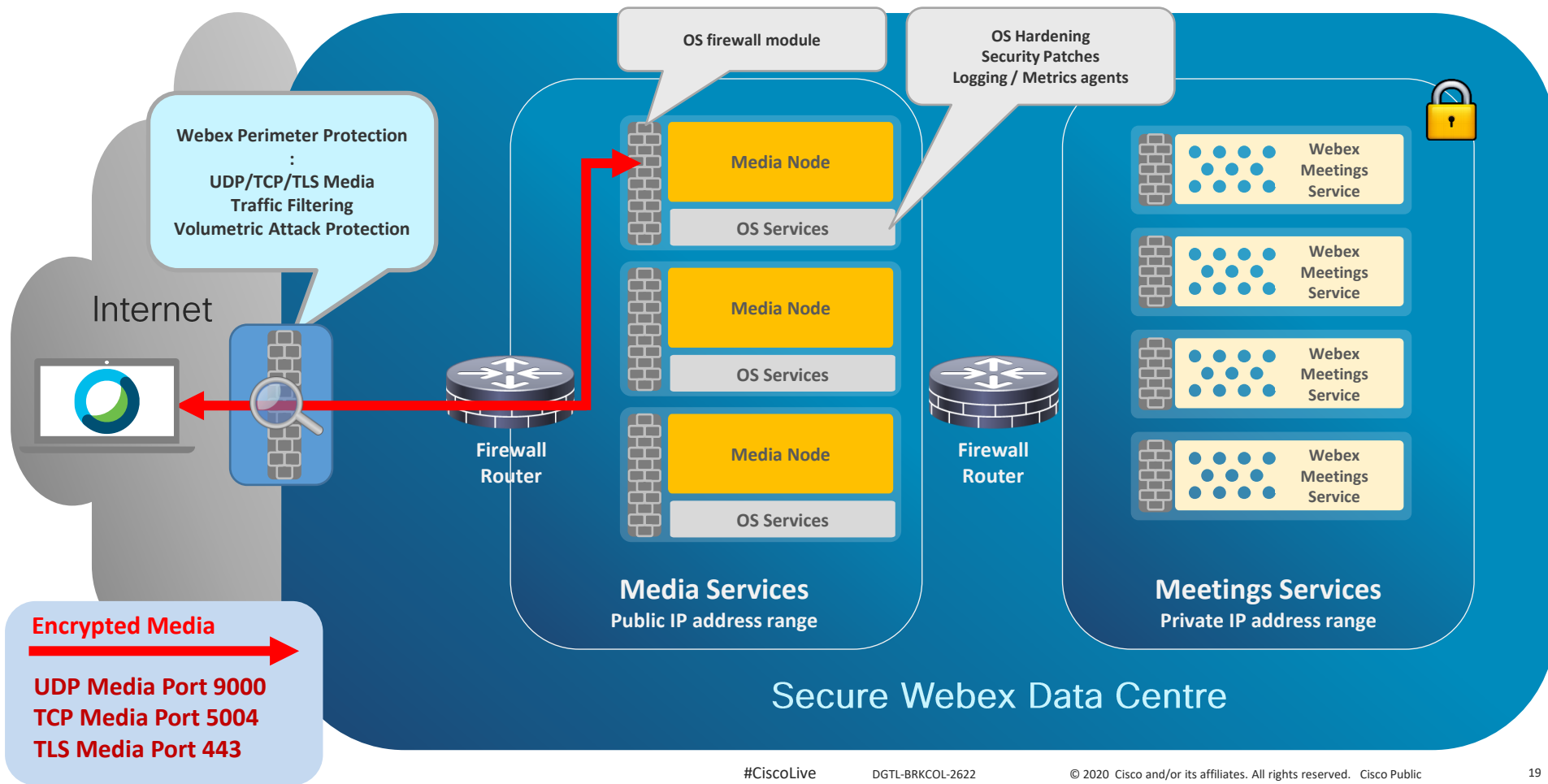


Webex Meetings Media Services



Webex Media services are globally distributed across multiple data centres
Media Server clusters in each data centre provide local and geographic redundancy
Media servers support voice, video and content sharing
All media is encrypted

Webex Media Services– Cloud Security and DMZ

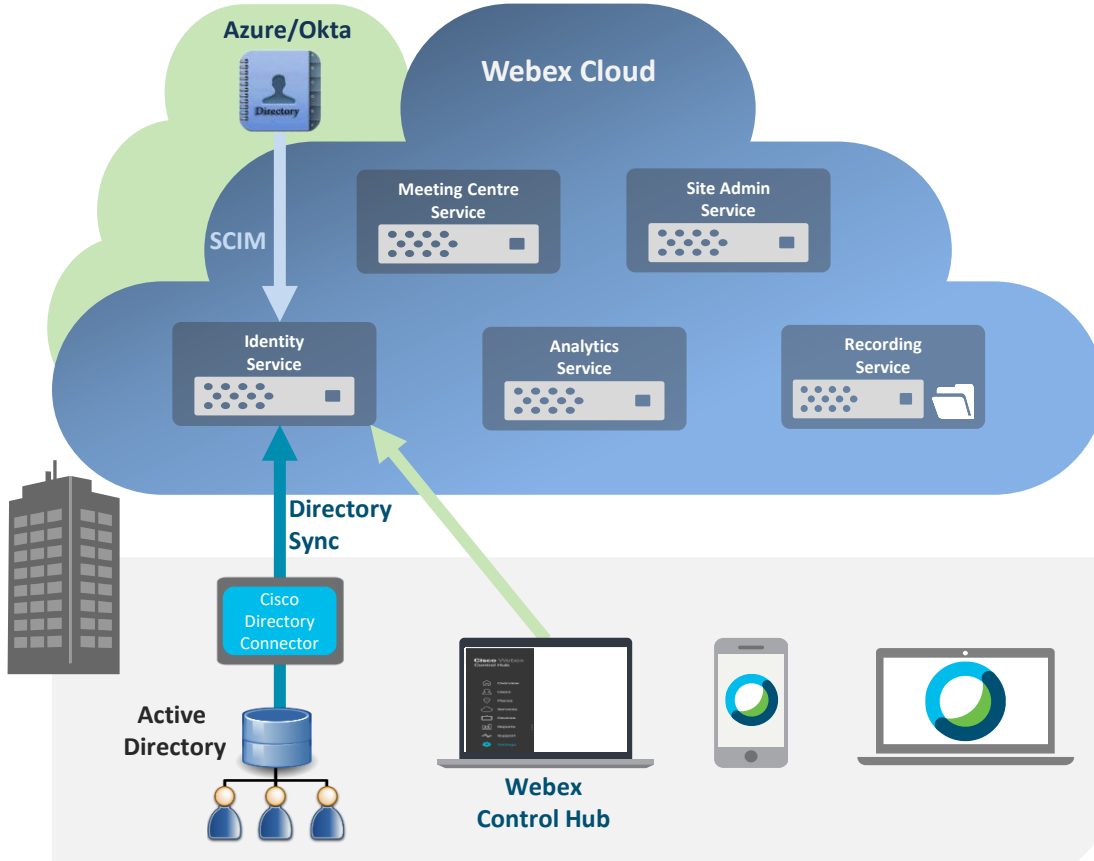


The background is a dark blue field filled with a dense pattern of small squares and dots in various shades of blue and orange. The squares are of different sizes, some appearing as larger, more prominent blocks while others are tiny specks. The dots are also of varying sizes, creating a textured, pixelated effect. The overall composition suggests a digital or network environment.

Webex Meetings :
Onboarding and Authenticating Users

Connecting to the cloud :
High Level overview for Apps & devices

Webex Meetings – User, Identity & Access Management

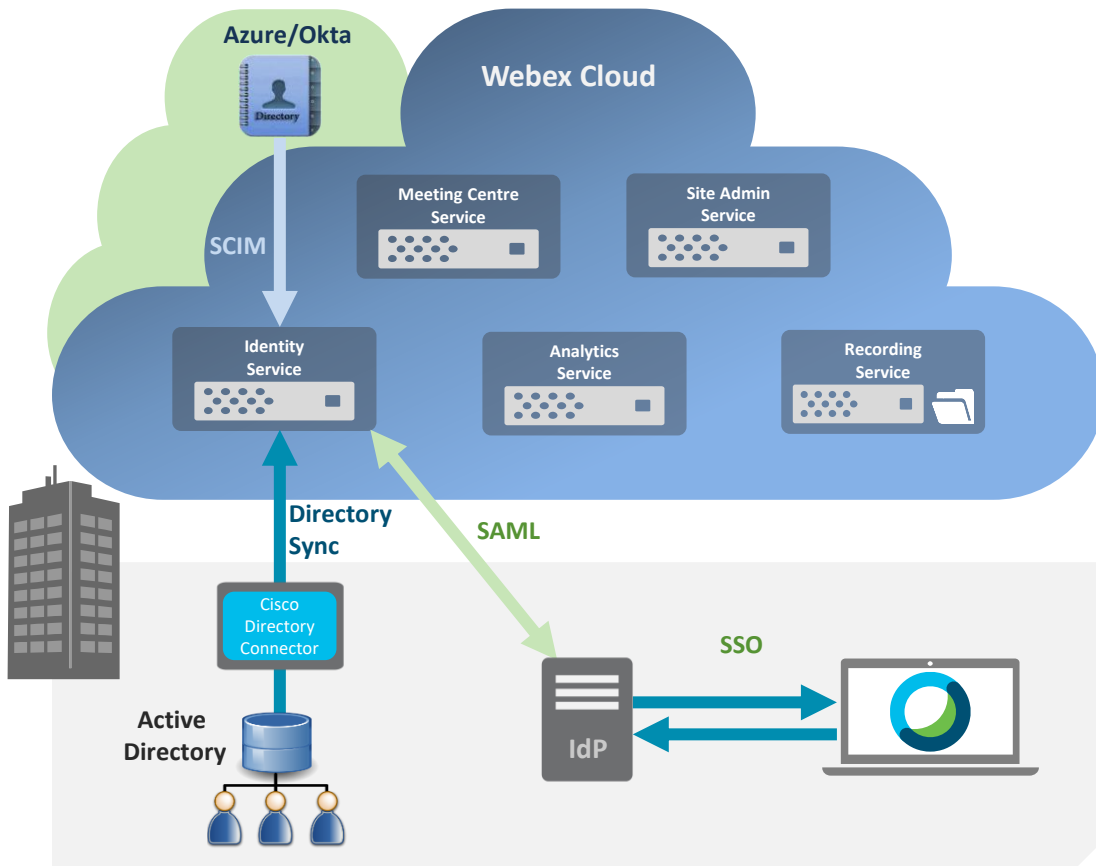


Webex Identity Service

User account creation methods:

- Webex Directory Connector
 - Active Directory Sync Tool
 - Control Hub only
- System for Cross-Domain Identity Management (SCIM) API
 - Sync from Cloud IdP
 - e.g. Azure AD, Okta User DB
 - Control Hub only
- Webex User/People API
- Manually add Users
- CSV File upload

Webex Meetings – SAML SSO Authentication



Single Sign On (SSO) for User Authentication :

Administrators can configure Webex Meetings to work with their existing SSO solution

Webex Meetings supports Identity Providers using Security Assertion Markup Language (SAML) 2.0 for Authentication and OAuth 2.0 Authorization

For list of supported IdPs see

<https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Cisco-Webex-Control-Hub>

Connecting to the Webex cloud – Apps and Devices

Cisco Webex Meetings Apps :

- Windows, Mac
- iOS, Android
- Web

Authentication – User Sign In

Authorization – OAuth 2.0

Cisco Webex Devices :

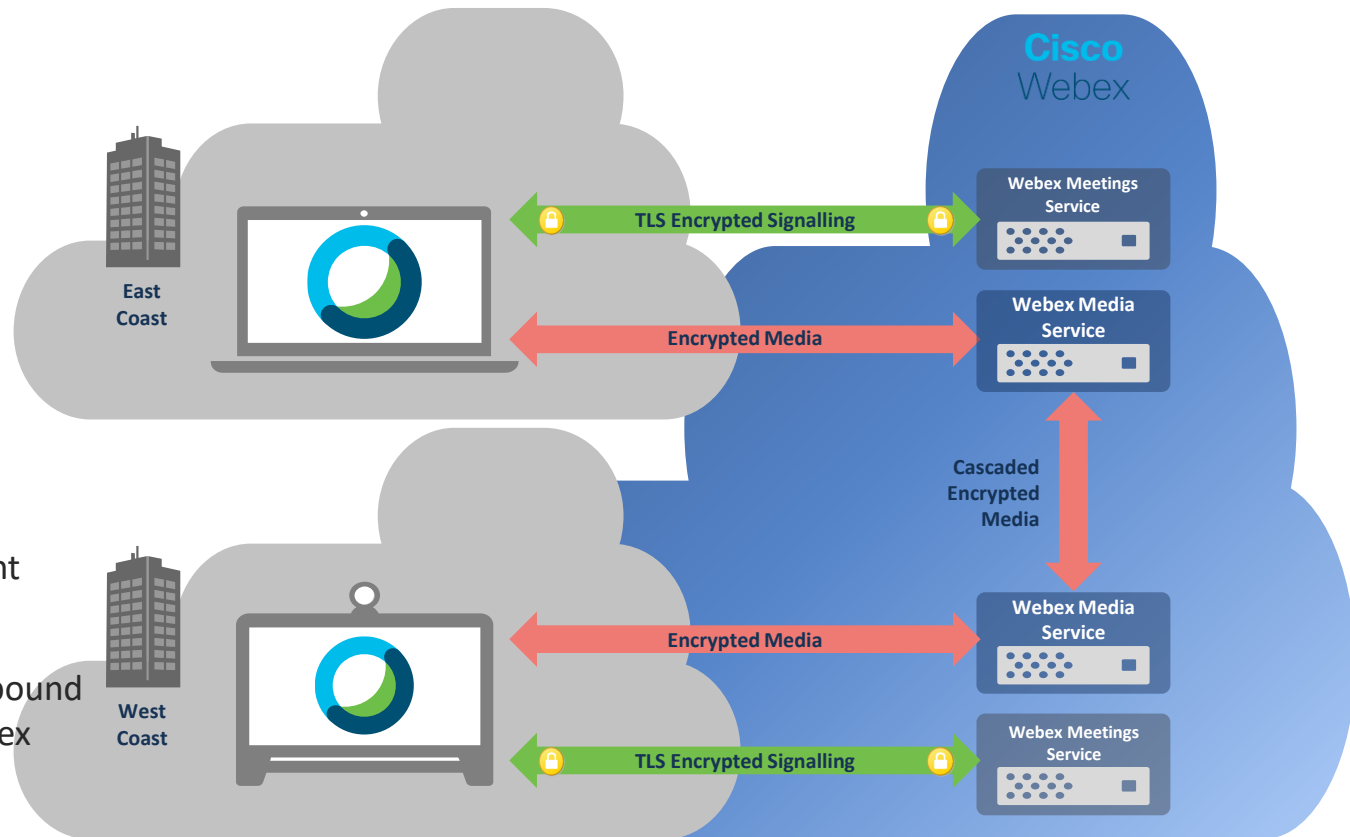
- Webex Room Series
- Webex Desktop Series
- Webex Board

Onboarding – Activation Code

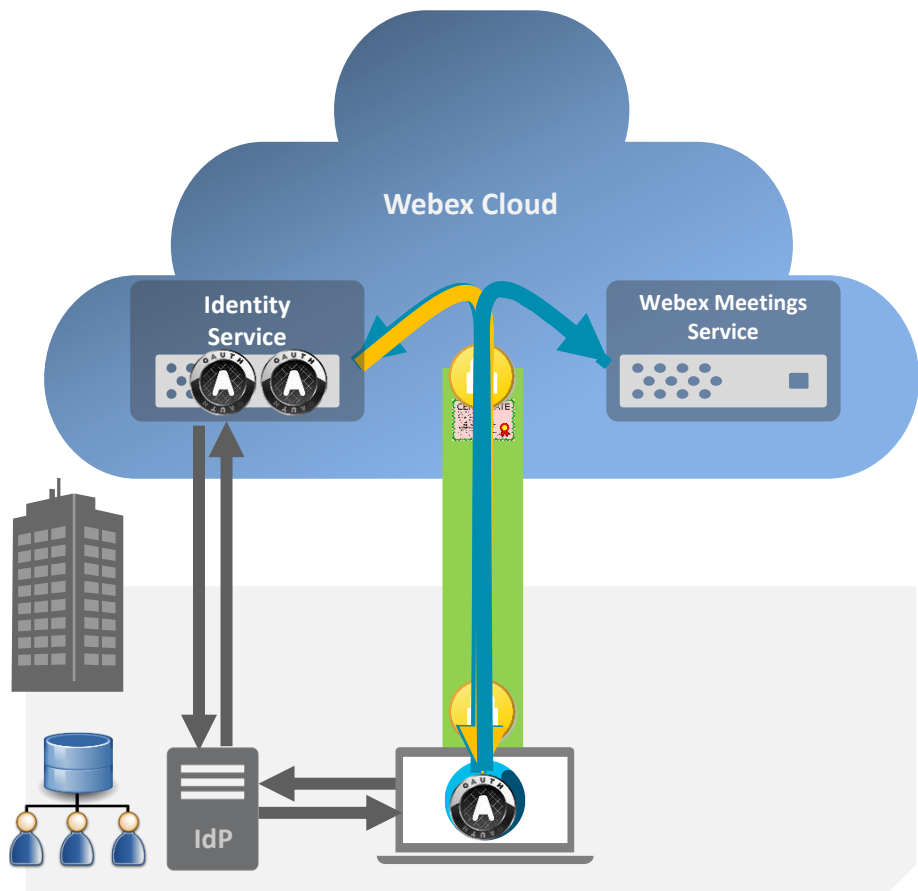
Authentication - Machine Account

Authorization – OAuth 2.0

All initiated connections are outbound only, from the Enterprise to Webex Cloud



Webex Meetings App – cloud connection - summary



- 1) Customer downloads and installs the Webex Meetings App
- 2) Webex Meetings App establishes a secure TLS connection with the Webex Cloud
- 3) Webex Identity Service prompts User for their Webex site URL e.g. `cisco.webex.com`
- 4) User Authenticated by Webex Identity Service, or Enterprise IdP (SSO)
- 5) OAuth Access and Refresh Tokens created and sent to Webex Meetings App
 - The Access Token contains details of the Webex Meetings resources the User is authorised to access
- 5) Webex Meetings App presents its Access Token to register with Webex Meetings Services over a secure channel

Webex - Device Onboarding

Webex Device application software and embedded OS installed as a firmware binary image before leaving the factory

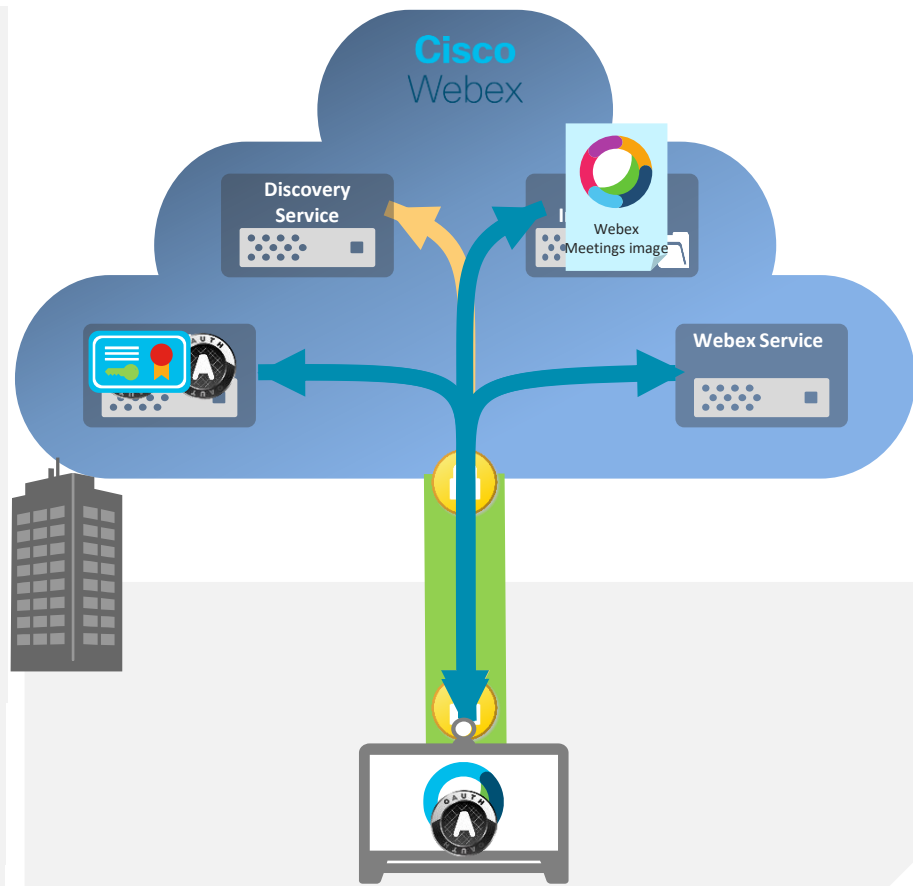
Webex Control Hub Admin generates device activation code for the device

User prompted for activation code during device installation. Activation code sent to Webex discovery service, which determines the device's organization and redirects to the Identity Service

Identity Service sends OAuth tokens and Trusted Root Certificate list (can include Enterprise CA Certs for TLS inspection) to device

Device checks current software version. If upgrade required, a signed image is sent to the device. Device will not load an unsigned image

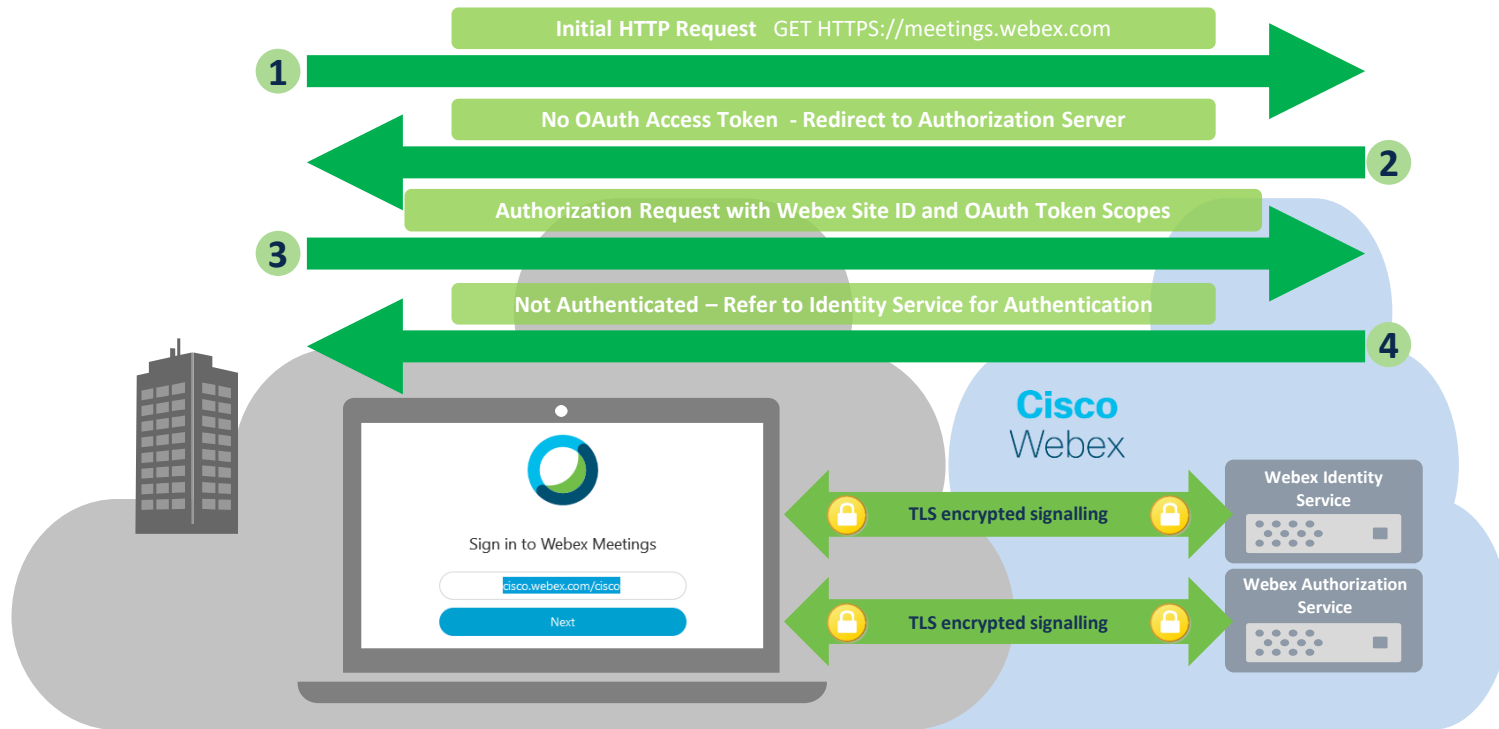
Device registers to Webex Services



Webex Meetings

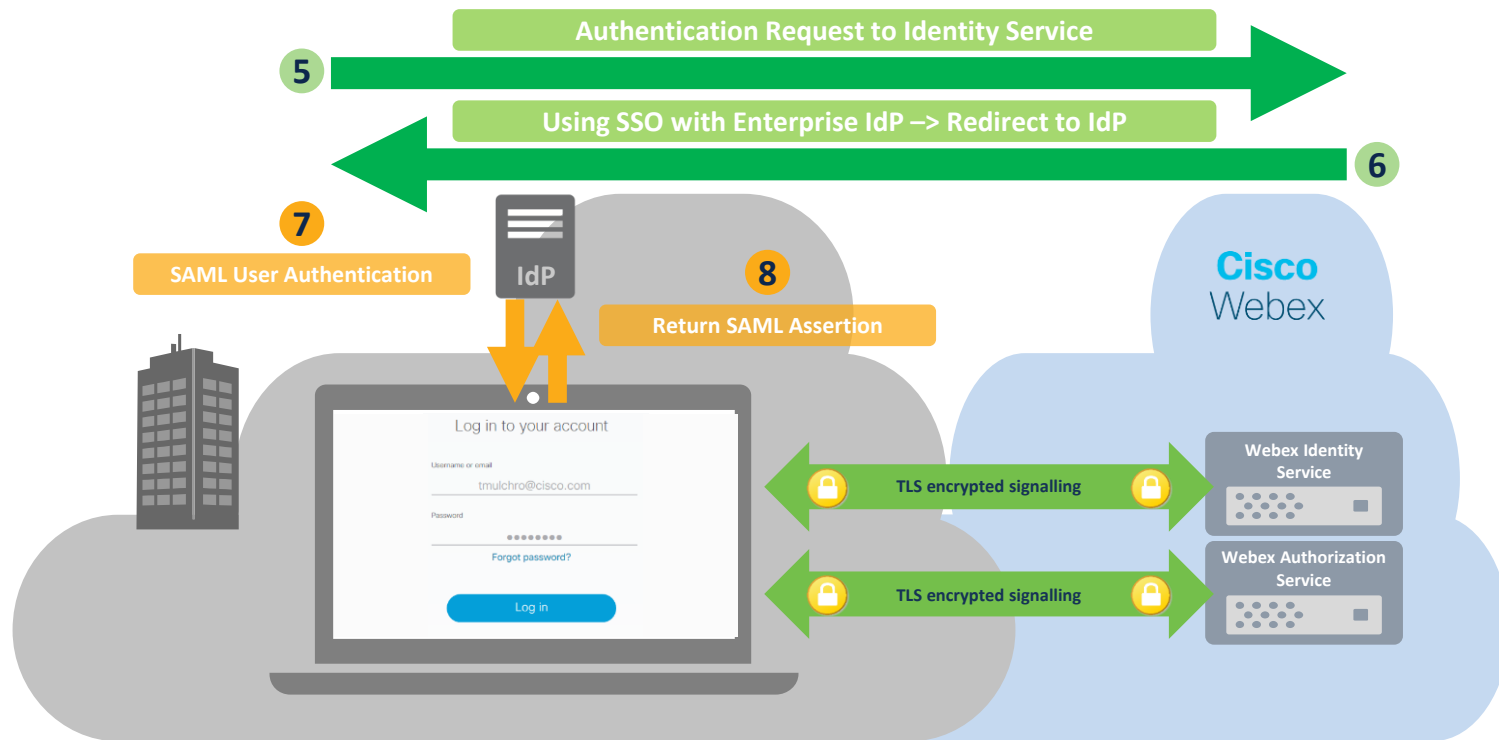
Authenticating Users
App/Device Authorization
OAuth Access & Refresh Tokens

Webex Meetings App : User Authentication (1)



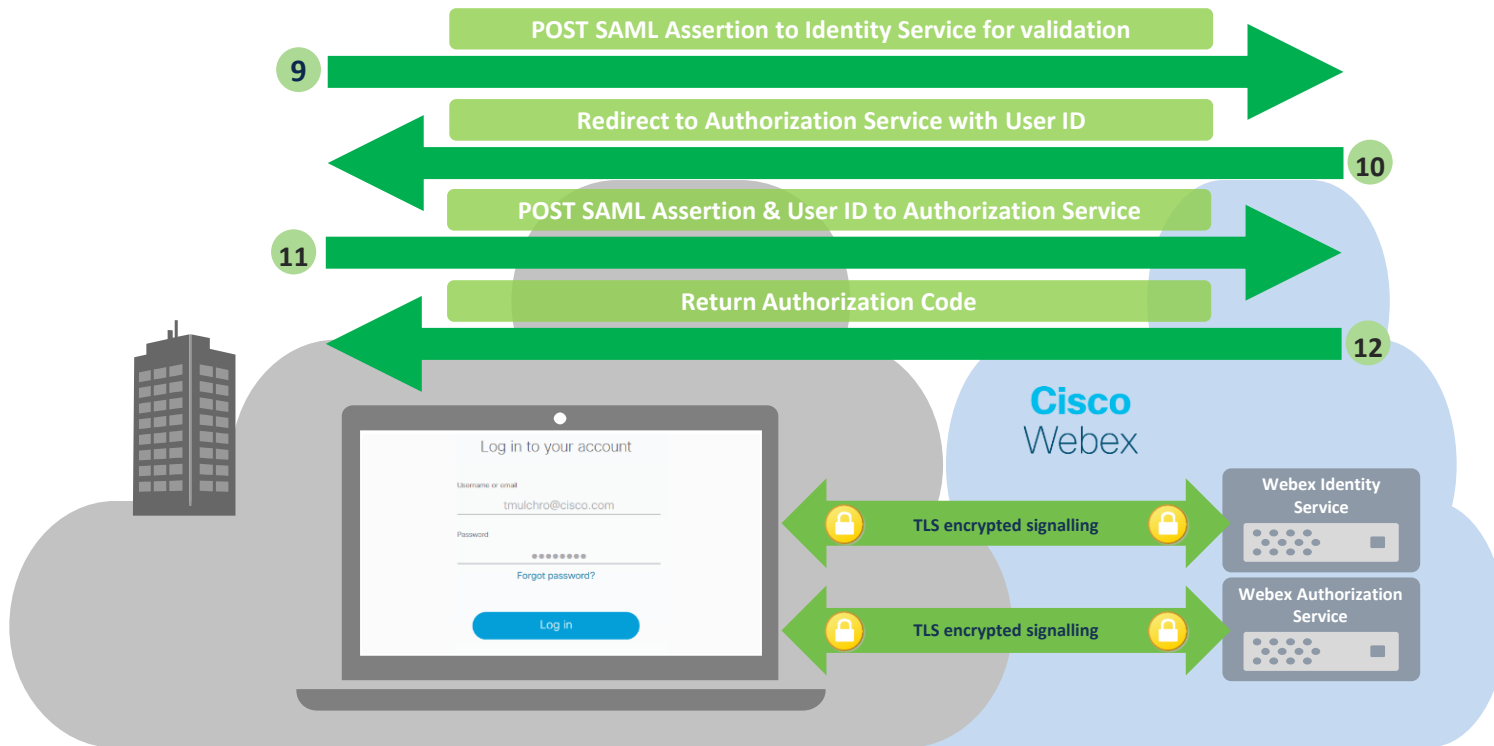
To access any Webex Meetings service – the App/ Device must present a validate OAuth Access Token
If no Access Token is present - the App/Device is redirected to the Authorization Service
The Webex Site ID in the Authorization request determines the User's Org and Identity Service
App/ Device redirected to Identity service for Authentication

Webex Meetings App : User Authentication (2)



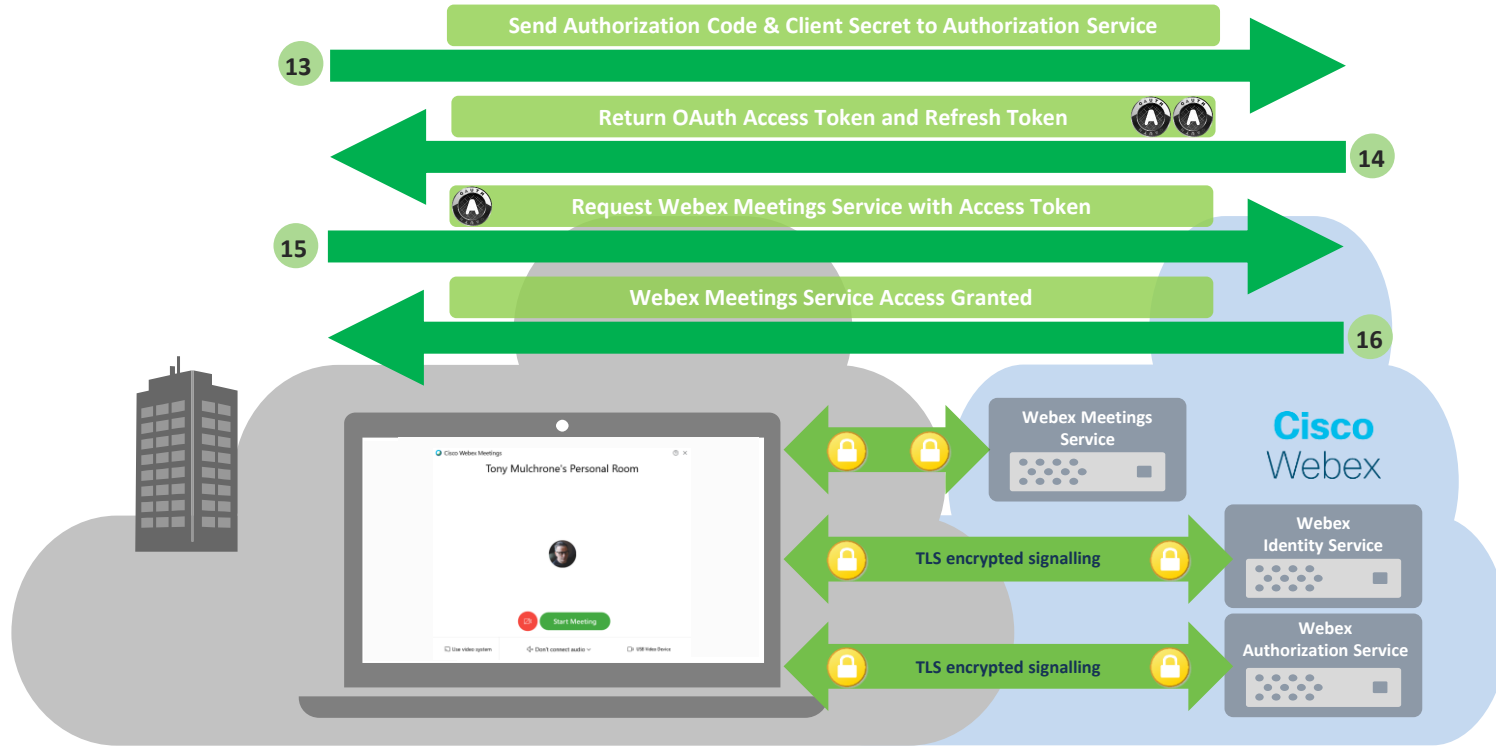
Users can Authenticate to the Webex Identity service (typically consumer accounts), or to an Enterprise (on-premises, or cloud) IdP that supports Single Sign on (SSO) using Security Assertion Markup Language version (SAML) 2.0 (as shown above)

Webex Meetings App : User Authentication (3)



Webex Meetings users using Single Sign On, use a combination SAML for authentication and the OAuth Authorization Code Grant method (as shown above), or Client Credential Grant method for authorization

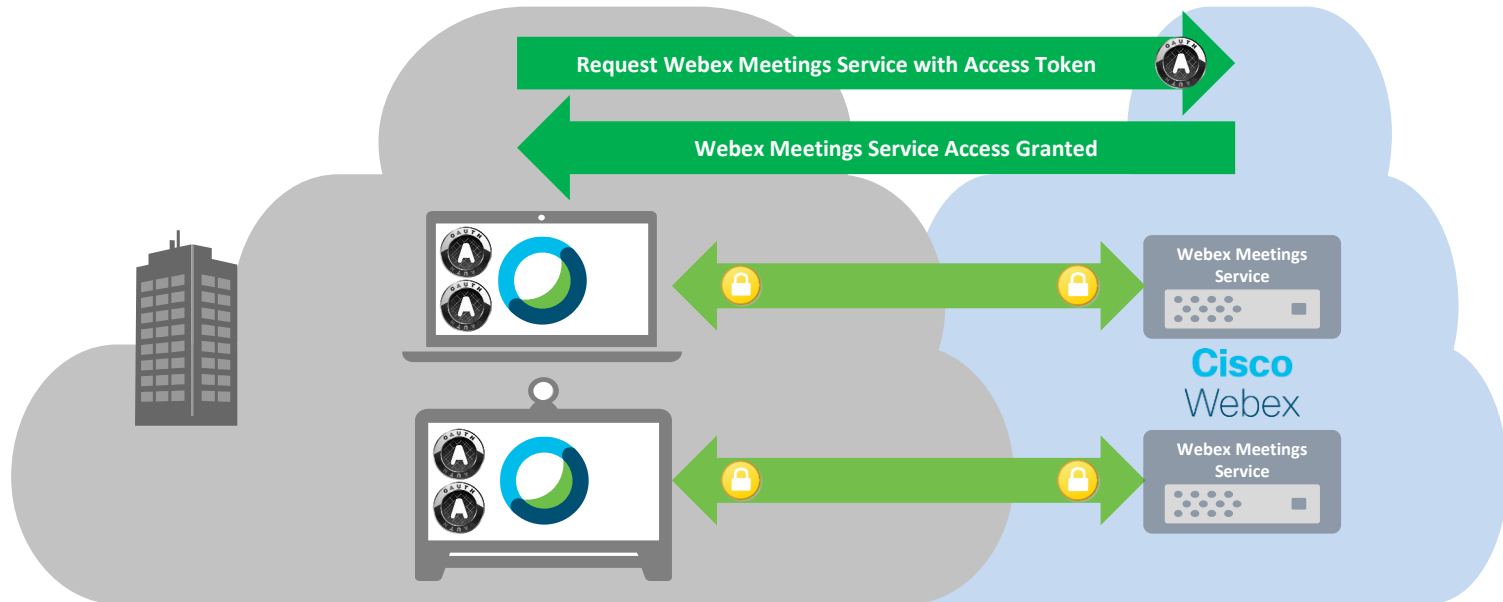
Webex Meetings App : User/Device Authorization



Once the Webex Meetings App/ Device is authenticated the OAuth Grant flow is used to deliver OAuth Access and Refresh Tokens to the App/ Device

The Access Token must be presented to gain authorized access to Webex services

Webex Meetings : OAuth Access and Refresh Tokens



OAuth Access Token – Uses JSON Web Token (JWT) format, signed (JWS)

OAuth Refresh Token – Presented to the authorization service to renew the Access token

Access tokens allow apps and devices to gain access to authorized services

Access tokens contain scopes that define which services are authorized

Access tokens are renewed when they reach 75% of their lifetime

Webex Meetings : OAuth Access and Refresh Tokens



Webex Access Token lifetimes vary by device e.g.

Meetings App access token lifetime = 6 hours

Device access token lifetime = 6 hours

Directory Connector access token lifetime = 1 hour

Access Token renewed by sending Refresh Token when lifetime = 75%

Token lifetime values can be reconfigured by service request



Webex Refresh Token lifetime typically 60 days

Lifetime values can be reconfigured by service request

Refresh Token renewed when Access Token renewed

Refresh Token renewal (on/off) configurable by service request

If Refresh Token renewal = Off : App logged-out, Device off-boarded when Refresh Token lifetime expires

OAuth Access Token scopes

Define which Meetings services Webex Apps and Devices are permitted to use e.g : Read User data, Read Meeting data, Read Recording data, Write User data, Write Meeting data, Write Recording data, Write Settings data

Webex Apps and Devices have more than one access token

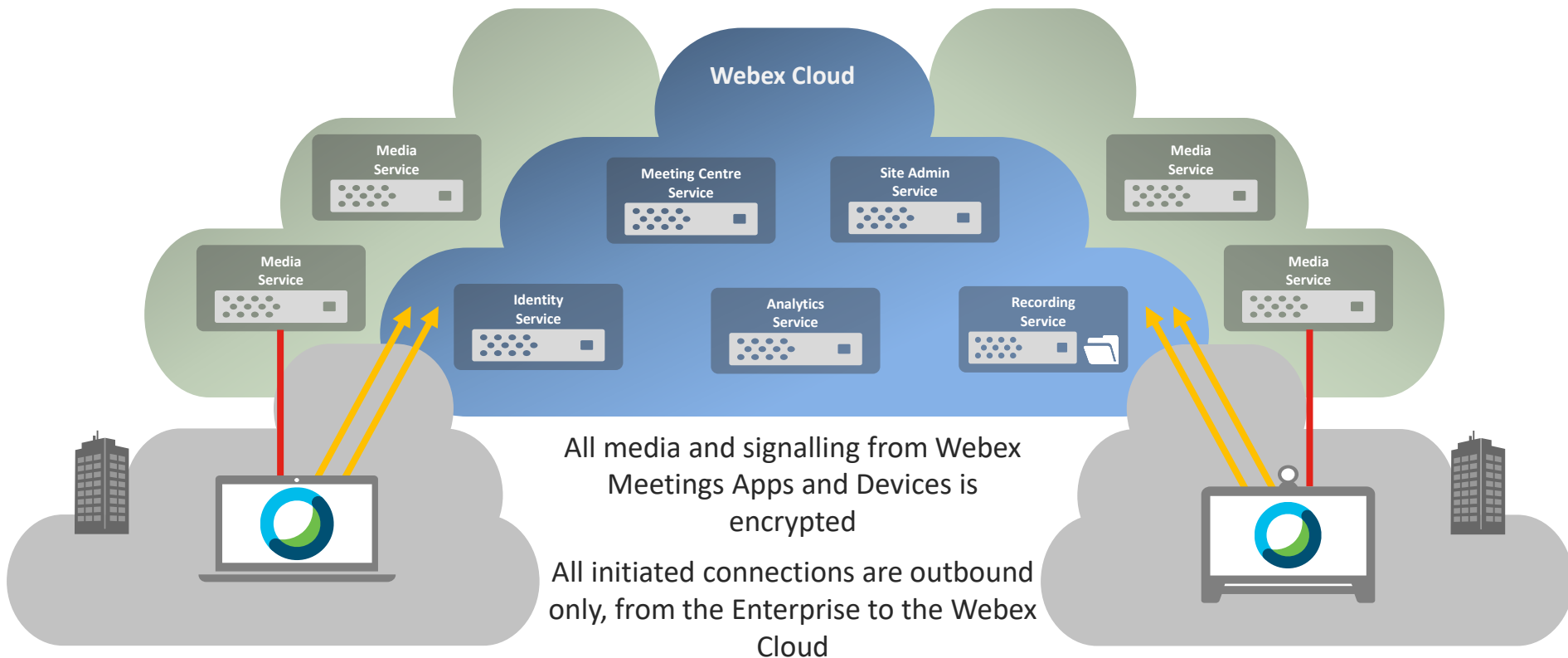
e.g. Webex Cloud Identity Services token, Webex Meetings Token



Secure Webex Signalling

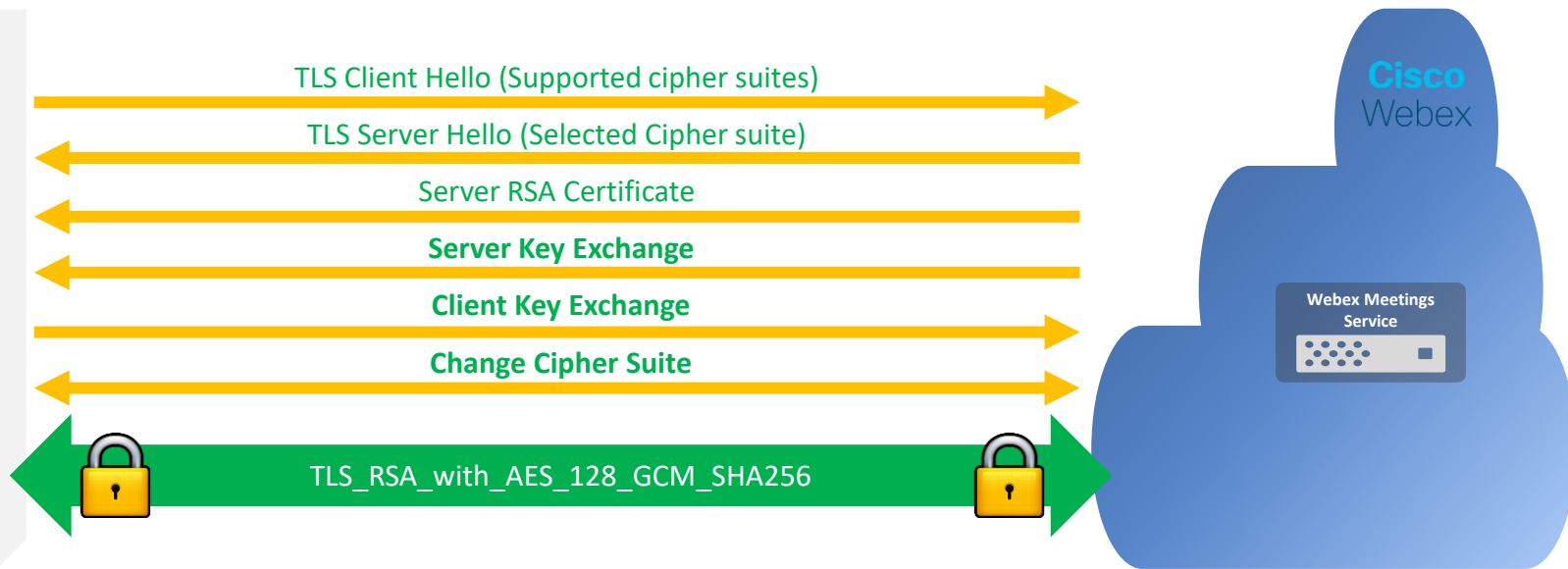
TLS Signaling Connections :
Authenticating Webex Services

Connecting to Webex Meetings Services



TLS 1.2 Encrypted Signalling : TLS_RSA_WITH_AES_128_GCM_SHA256

Webex Meetings TLS negotiation

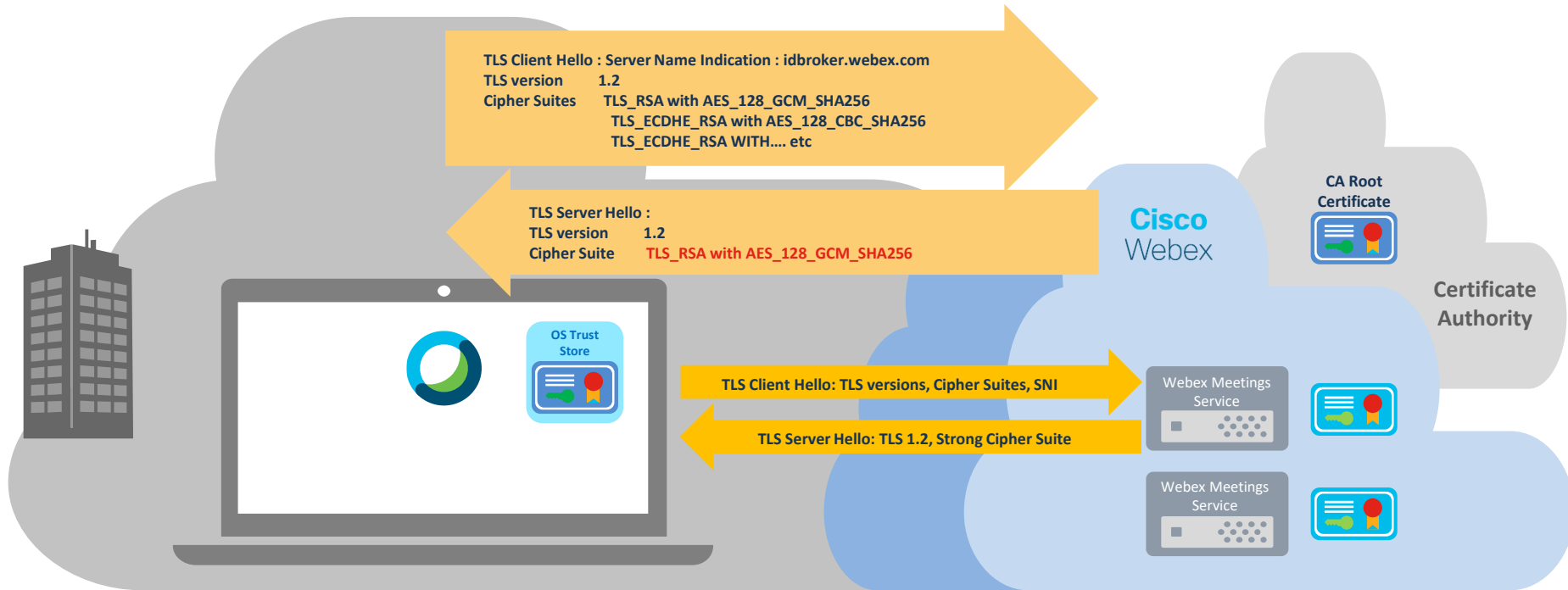


Webex Meetings : TLS version 1.2 only with the following cipher suites in preference order :

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- See notes for complete list of TLS Ciphers

ECDHE : Key Negotiation with Forward Secrecy
RSA : Certificates (2048 bit key size)
AES_256 : NSA Top Secret Encryption Strength
AES_128 : NSA Secret Encryption Strength

Webex Meetings: TLS Client and Server Hello Cipher Suite negotiation



Certificate Trust store for Webex certificate validation

Webex Meetings Apps : Root CA Certificate in OS Trust store

Webex Devices : Root CA Certificate downloaded to device trust store during onboarding

Validate Webex Certificate Chain :

- ✓ Certificate Name
- ✓ Certificate Lifetime
- ✓ Certificate Issuer
- ✓ Key Size
- ✓ Signature Algorithm
- ✓ Revocation status

OS Trust Store

CA Root Certificate

Certificate Authority

Webex Meetings Service

Webex Meetings CA Signed Certificate

Root and Intermediate Certificates

Cisco Webex

CA signed server cert, CA Root cert, and any intermediate certs are sent to the Webex App/Device

The Webex App/Device verifies the following in each certificate :

Digital Signature/ Certificate Issuer/ Certificate Validity Period/ Certificate Revocation status/ Key Size/ Key Usage
Certificate Extensions/ Server Hostname

Webex Meetings : Service Certificate validation

CA Root Certificate

Subject : **Root Cert Auth**

Common Name : Root Cert Auth

Subject Alt. Name

Valid From : 01 Jan 2010

Valid Until : 29 July 2035

Issuer : **Root Cert Auth**

CA Authorized OCSP Responder

Signature Algorithm : SHA-1 with RSA

Digital Signature Value : 1111

RSA Public Key Size : 2048 bits

RSA Public Key Value : 1234567890...

Intermediate Certificate

Subject : **Secure Cert Auth**

Common Name : Secure Cert Auth

Subject Alt. Name

Valid From : 02 Feb 2015

Valid Until : 28 June 2030

Issuer : **Root Cert Auth**

CA Authorized OCSP Responder

Signature Algorithm : SHA-256 w/ RSA

Digital Signature Value : **2222**

RSA Public Key Size : 2048 bits

RSA Public Key Value : 0099887766...

Server Certificate

Subject : identity.webex.com

Common Name : identity.webex.com

Subject Alt Name : *.identity.webex.com

Valid From : 23 Jul 2018

Valid Until : 23 Jul 2020

Issuer : **Secure Cert Auth**

CA Authorized OCSP Responder

Signature Algorithm : SHA-256 w/ RSA

Digital Signature Value : **3333**

RSA Public Key Size : 2048 bits

RSA Public Key Value : 1122334455...

SHA-256

2222

#CiscoLive

SHA-256

3333

DGTL-BRRCOL-2622

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

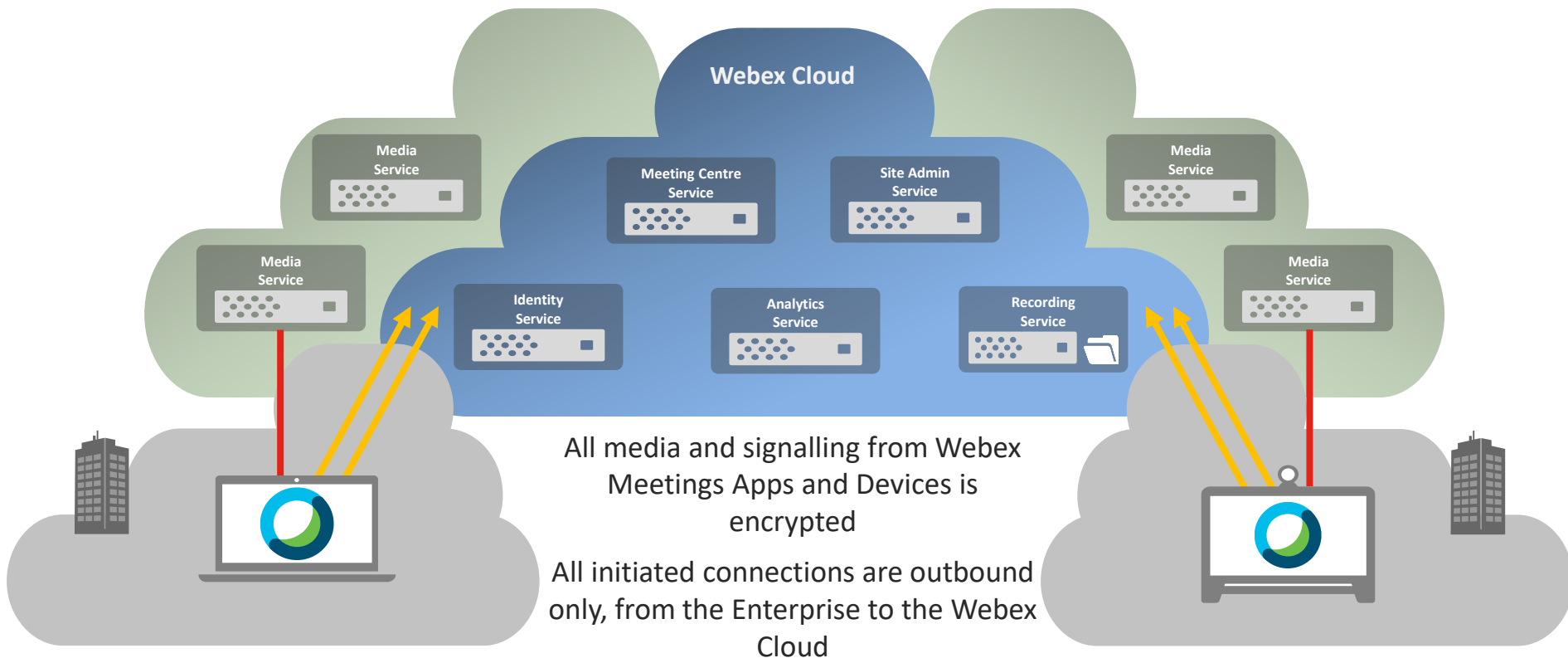
38

The background is a dark blue field filled with numerous small squares and dots in shades of blue and orange. These elements are scattered across the frame, with a higher concentration of orange squares and dots forming a diagonal streak from the top left towards the bottom right.

Webex Cloud Security

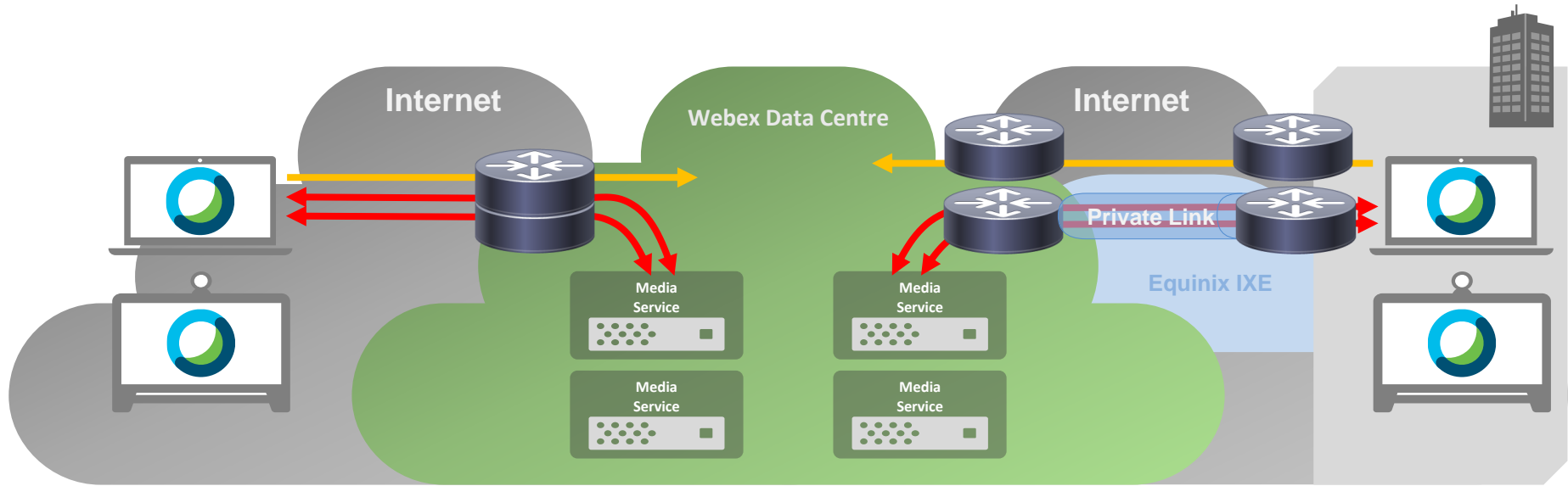
Encrypting Media :
Voice, Video & Content
End to End Media Encryption

Connecting to Webex Meetings Services



Encrypted Media : AES_CM_128_HMAC_SHA1_80/ AES_128_CBC/ AES_256-GCM

Access to Webex Meetings Media Services (1)



Webex Meetings Application and Webex Devices

Encrypted HTTPS Signalling
Encrypted Voice, Video and Content Sharing

Access Options

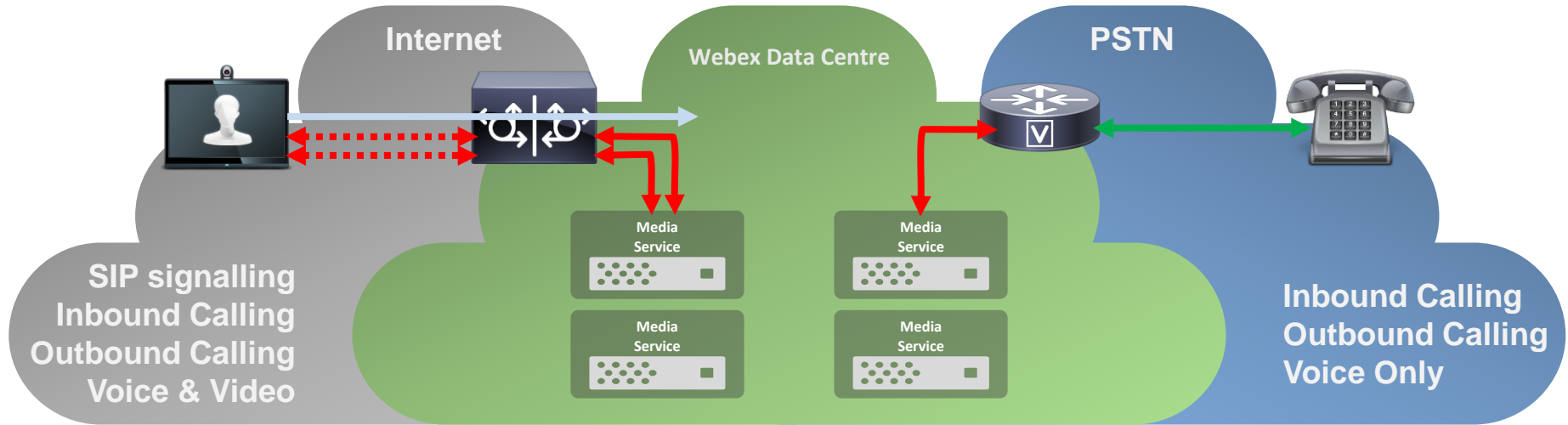
Internet Access

Signalling and Media traverse the Internet

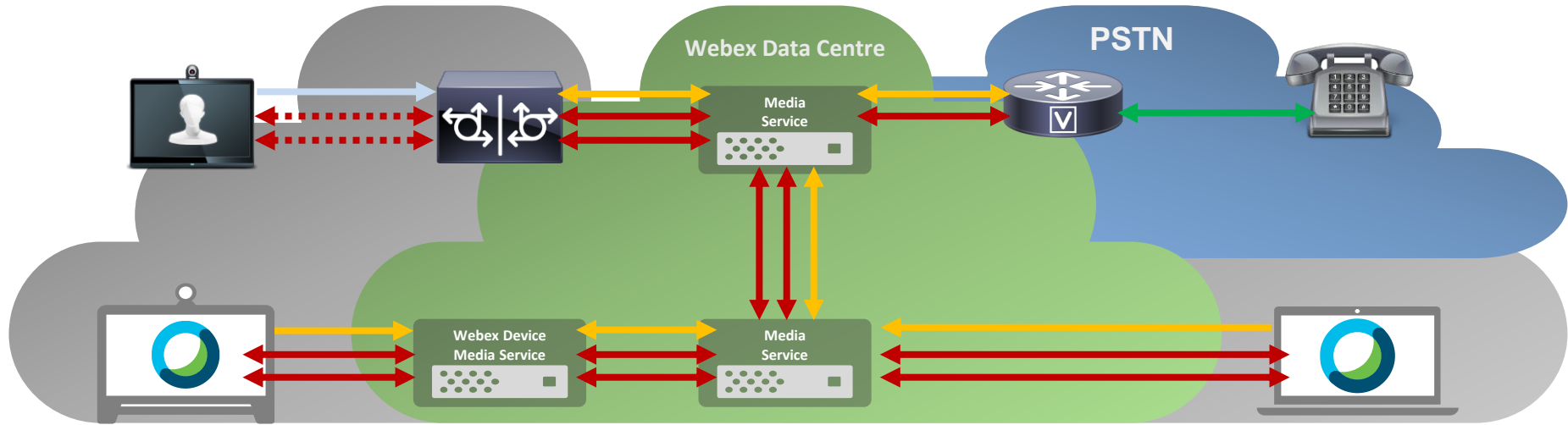
Private Peering

Media traverses Equinix Private Link
Non Webex App signalling traverses Internet

Access to Webex Meetings Media Services (2)



Standard Webex Meetings

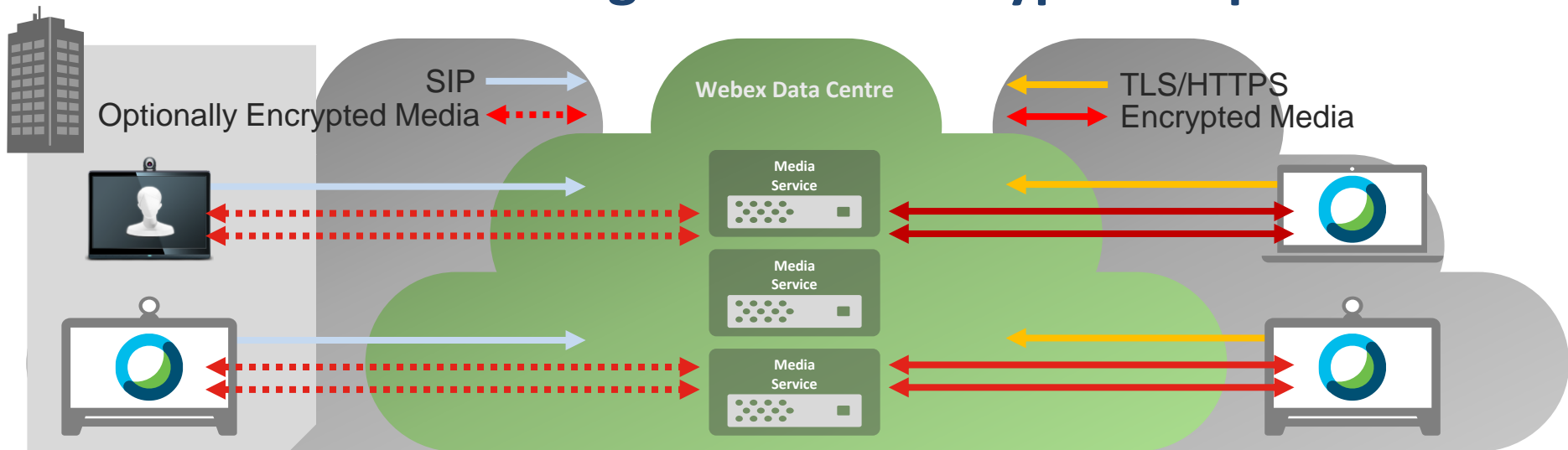


Standard Webex Meetings allow users to join via :

- Webex Apps**
- Webex Devices**
- SIP Voice and Video Devices**
- PSTN**

← TLS/HTTPS
← SIP
↔ Encrypted Media
↔ Optionally Encrypted Media
↔ Unencrypted PSTN audio

Webex Meetings - Media Encryption ciphers



3rd Party SIP devices
Media Encryption optional
AES-CM-128-HMAC-SHA1 cipher

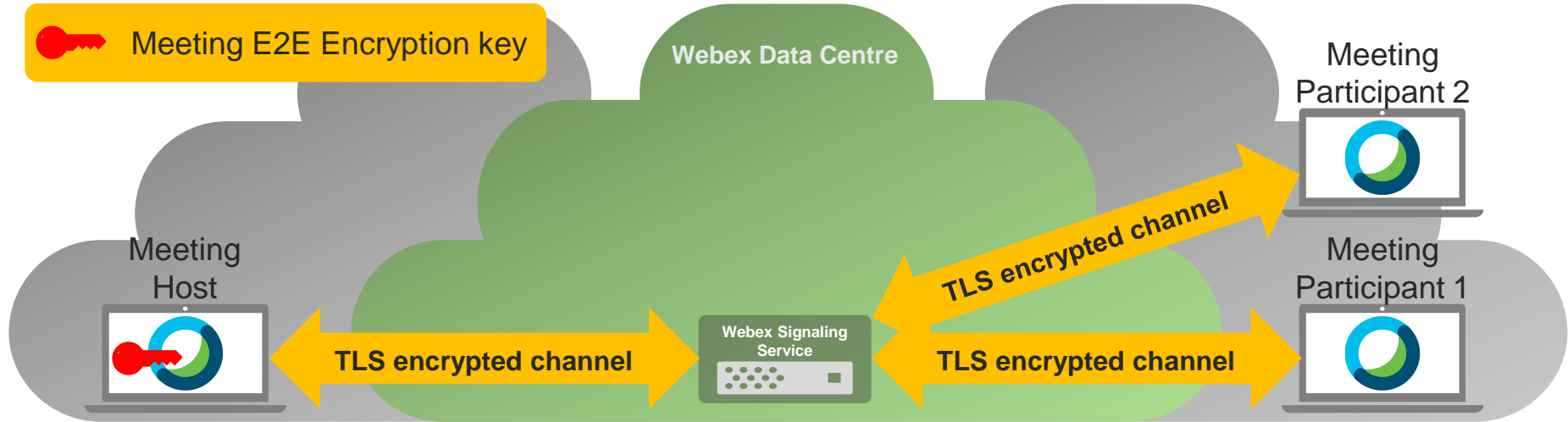
On Premises registered Cisco Devices
Media Encryption optional
AES-CM-128-HMAC-SHA1 cipher

Webex App
Media Always Encrypted
AES-128-CBC
AES-256-GCM*

Cloud Registered Webex Device
Media Always Encrypted
AES—CM-128-HMAC-SHA1 cipher

* AES-256-GCM media encryption - roll out planned for end of May/ early June 2020

Webex Meetings Apps – Strong End to End Encryption

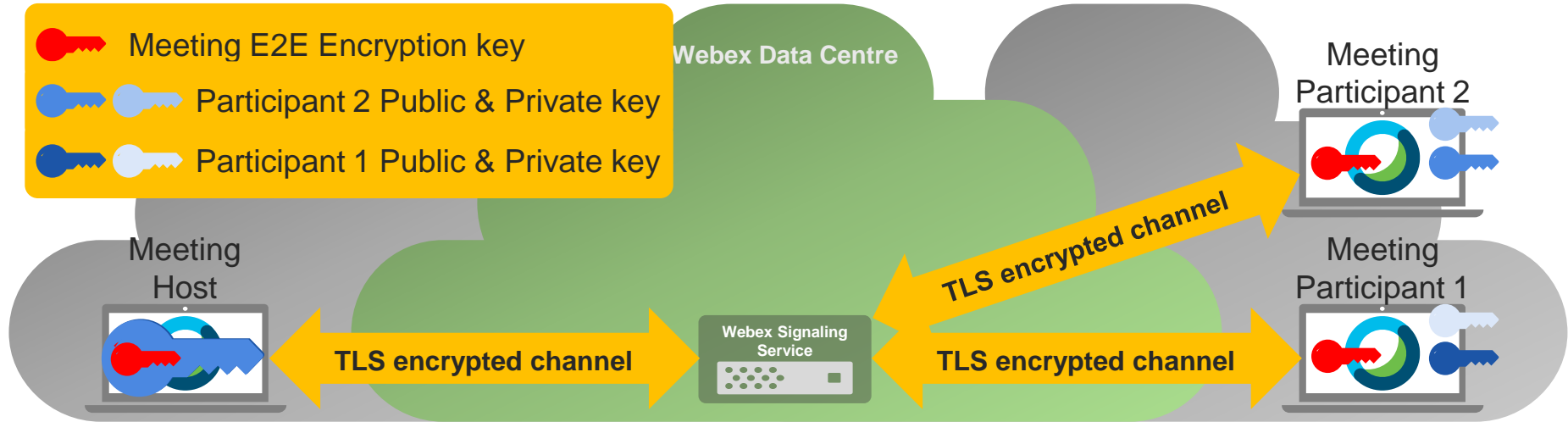


With End to End Encryption for Webex Meetings - Webex servers do not have a copy of the encryption key used by the meeting participants and cannot decrypt any meeting data.

End to End Encryption is only supported by the Webex Application (desktop & mobile apps)

The master End to End Encryption key is generated by the meeting host. Each participant's Webex App establishes a secure connection with the meeting host's Webex App to retrieve the end to end encryption key for the meeting

Webex Meetings Apps – Strong End to End Encryption



Each participant's Webex App generates a 2048 bit RSA public and private key pair

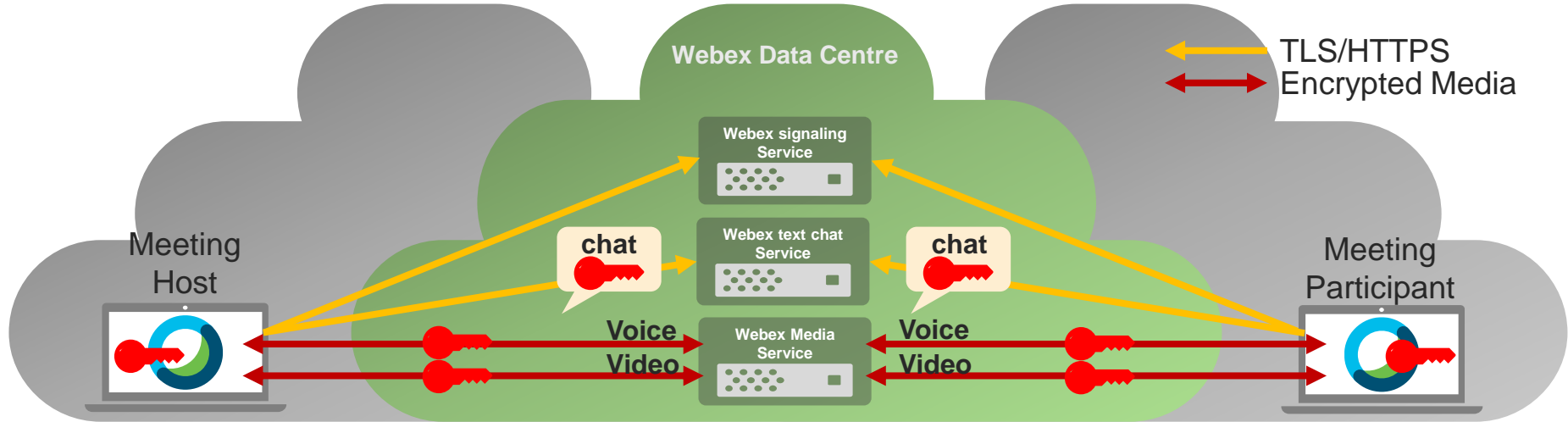
The public key is sent to the meeting host over TLS

The meeting host uses the participant's public key to encrypt the Meeting E2E encryption key and returns the encrypted key to the participant over TLS

Using this method to exchange the meeting E2E encryption key excludes it use by SIP endpoints, PSTN participants and recording services

i.e. E2E meeting encryption is supported by Webex Meetings Apps only

Webex Meetings Apps – Strong End to End Encryption



With Strong End to End Encryption - Webex servers do not have a copy of the E2E encryption key used by the Webex Application to encrypt meeting data.

The media is switched un-decrypted by the media server based on the speaker volume, which is indicated in the unencrypted packet header

Encrypted chat messages are distributed to all participants over encrypted TLS channels



Webex Meetings

Recording Services

Transcription Services

Webex Meetings : Network Based and Local Recording

Meeting Host Recording entitlements

Start recording in meeting

Automatically start recording when the meeting starts

Record Audio & content only, or Audio, Video & content

Recorded meeting file editing options: Include/Exclude :
Chat, Q&A, Polling, Participants, Transcripts

Site Admin Meeting Recording options

Recordings can be password protected

Recordings can be streamed or downloaded

Downloading of recordings can be blocked

Viewing can be restricted to signed in users only

Network Based Recordings

Stored in regional Webex Data Centers

Encrypted using AES-256-GCM

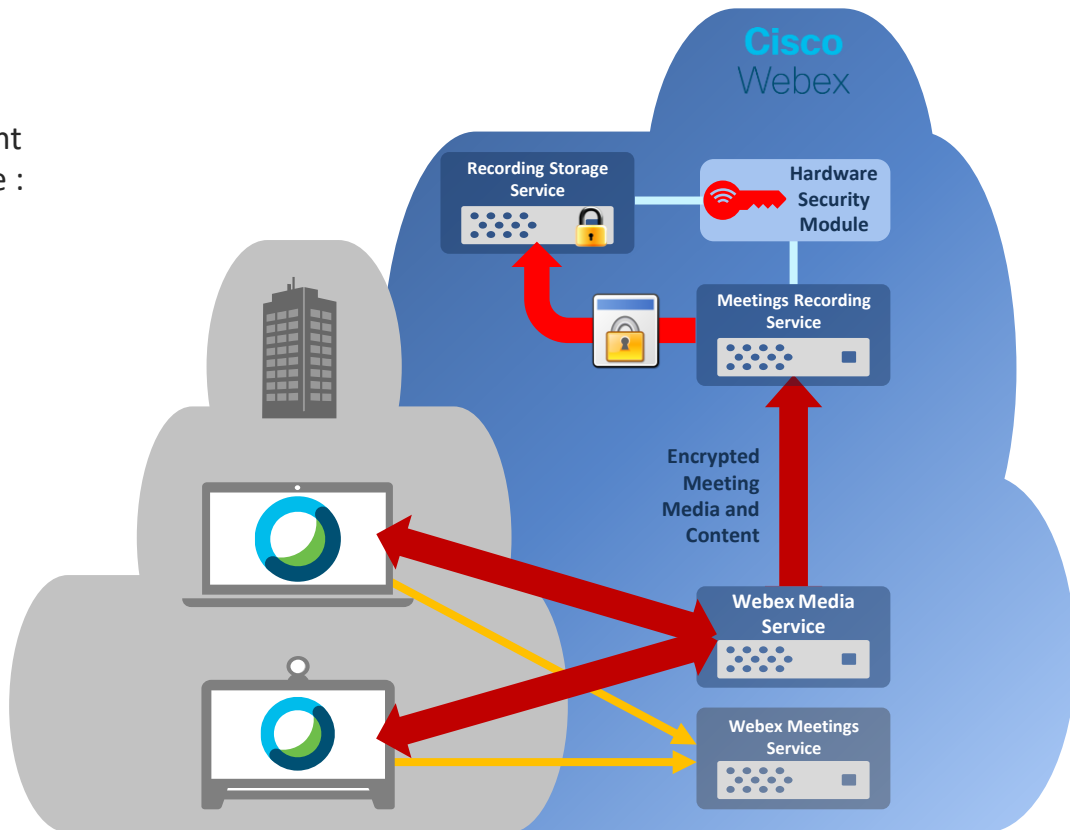
Master key stored in HSM

Configurable Retention period

Local Recording

Optionally enabled by site Admin

Meeting saved on host's computer as MP4 or WRF



Webex Meetings : Meeting Transcription Service

Meeting Transcription

Transcripts produced from meeting recordings

Transcripts can be searched

Transcripts can be edited

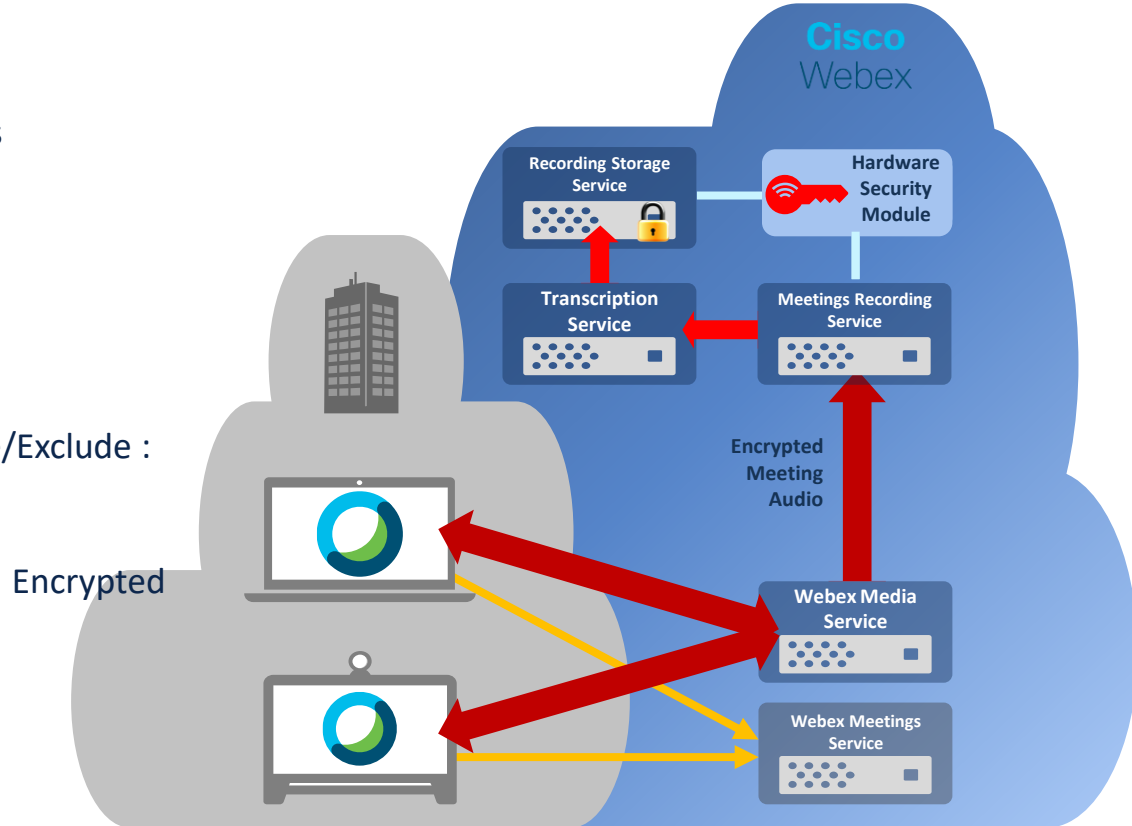
Transcripts are bundled with recording files

Recordings can be password protected

Recorded meeting file editing options: Include/Exclude :
Chat, Q&A, Polling, Participants, Transcripts

Transcripts stored in regional Webex DCs
using AES-256-GCM

Master keys stored in HSM



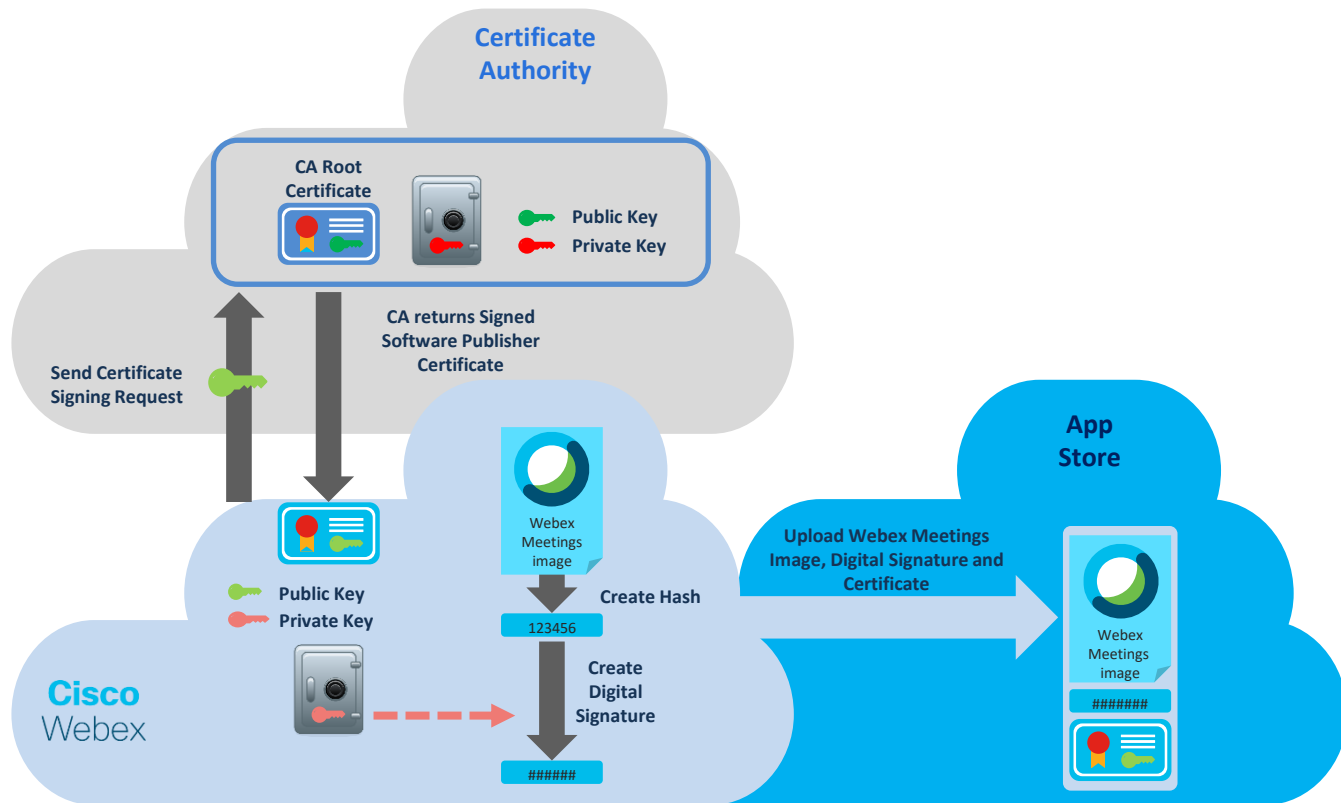
Webex Meetings App Security

Software verification Encryption of
data at Rest
Proximity
Cognitive Collaboration

Webex Meetings Apps – Co-signed software images

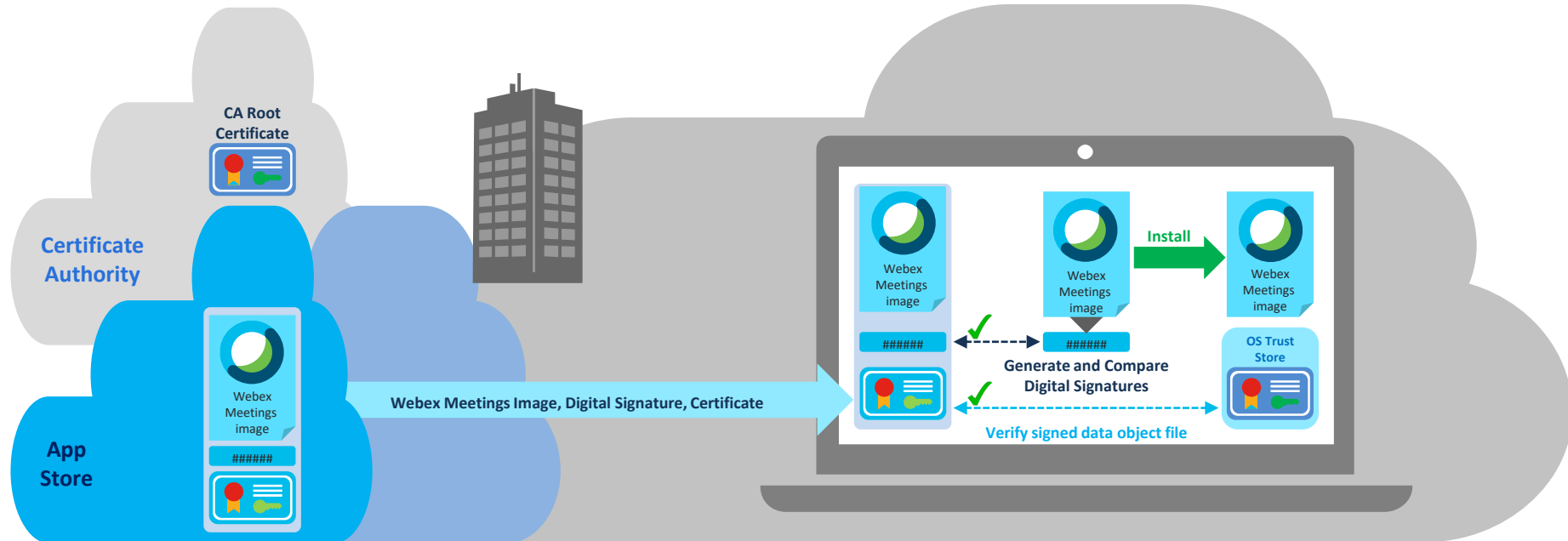
Cisco uses a CA-signed software publishing certificate to digitally sign the Webex Meetings software image.

And then uses the code-signing infrastructure of each platform vendor (Microsoft/Apple/Google) to co-sign a PKCS #7-signed data object file containing the signed Webex Meetings image, digital signature, and software publishing certificate.



Webex Meetings App: Software image verification

When a user downloads the Webex Meetings software image, the platform operating system verifies the digital signature PKCS #7-signed data object file and then verifies the digital signature of the Webex Meetings image



Webex Meetings Apps : Encryption of Data at Rest

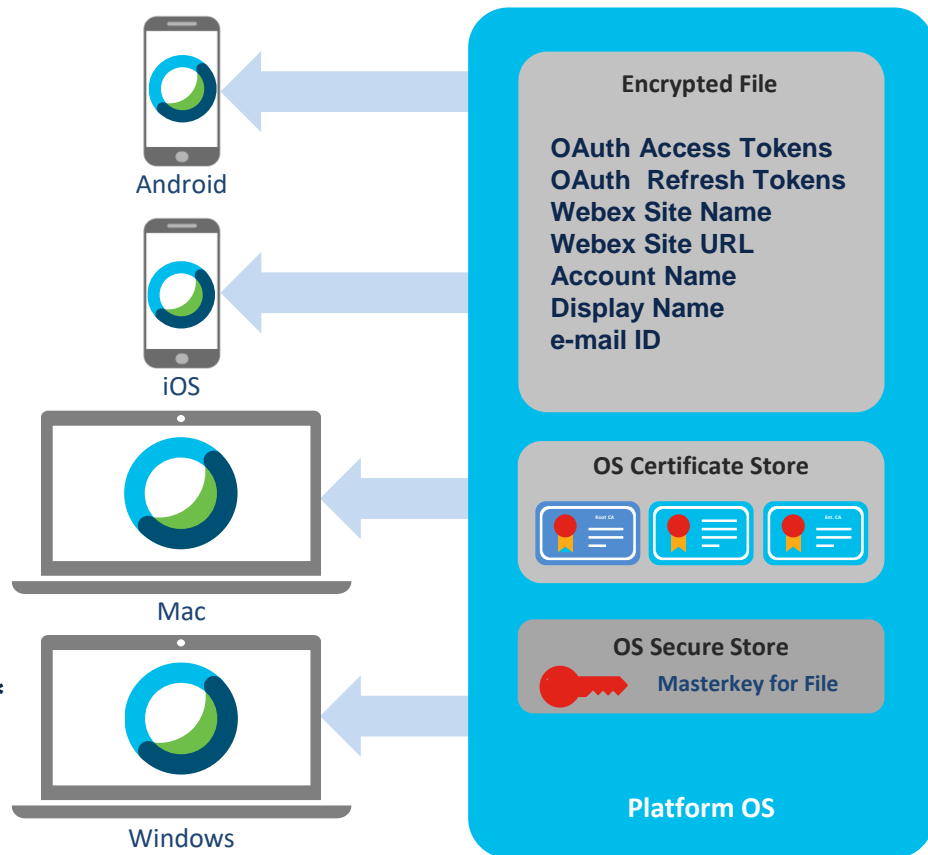
Webex Meetings Apps do not persist user generated meeting content i.e.:

- Chat messages
- Files
- Recordings (Recordings can be stored locally)
- Media Encryption keys

Webex Meetings Apps do store and encrypt :

- OAuth Access and Refresh Tokens
- Webex Site Name and URL
- Account Name
- Display Name
- e-mail ID

Stored Webex data is encrypted using an **AES-256*** encryption key
Master Key stored in OS secure Store



Secure Cloud Registered Webex Devices

Webex Devices :

- Webex Room Series
- Webex Desktop Series
- Webex Board

Onboarding – Activation Code

Authentication - Machine Account

Authorization – OAuth 2.0

REST based Signaling Transport : TLS version 1.2 Only

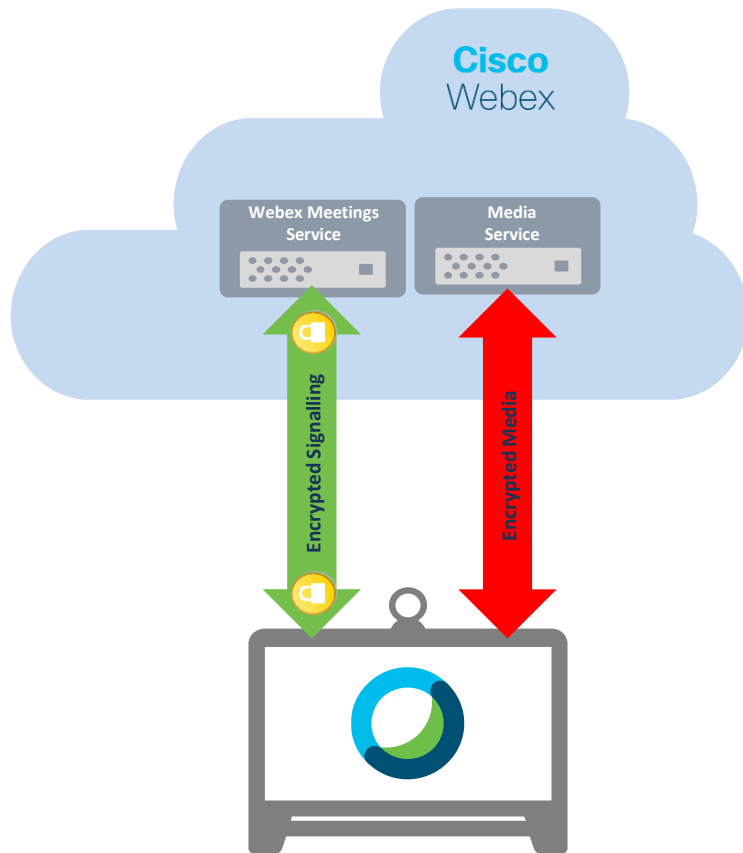
Negotiable Ciphers with Webex Services :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

SRTP Media Encryption cipher : AES-CM-128-HMAC-SHA1

Media Transport protocols : UDP/TCP/TLS

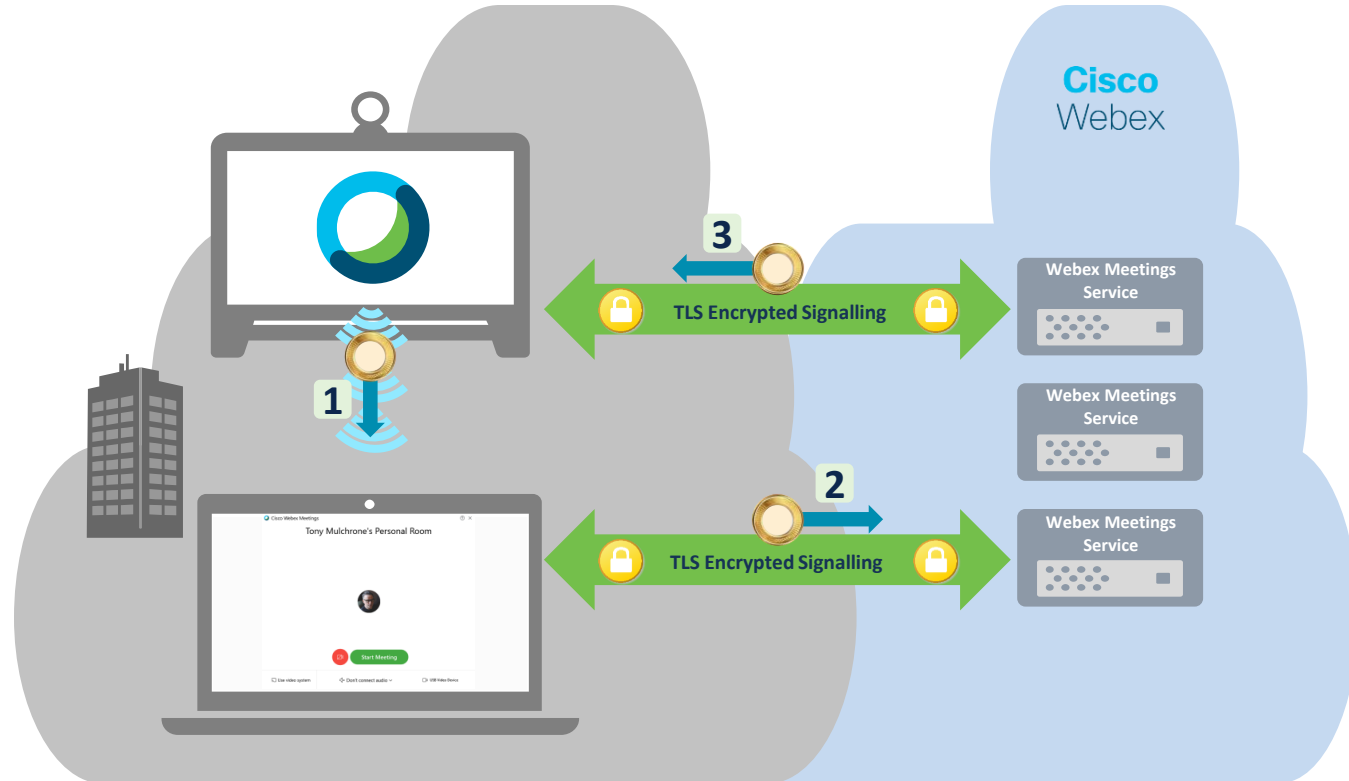
RoomOS software – digitally signed and verified



Webex Meetings App and devices Proximity – Device detection and pairing

Cloud-registered Webex devices use ultrasonic signalling and tokens to discover and pair with Webex Meetings apps

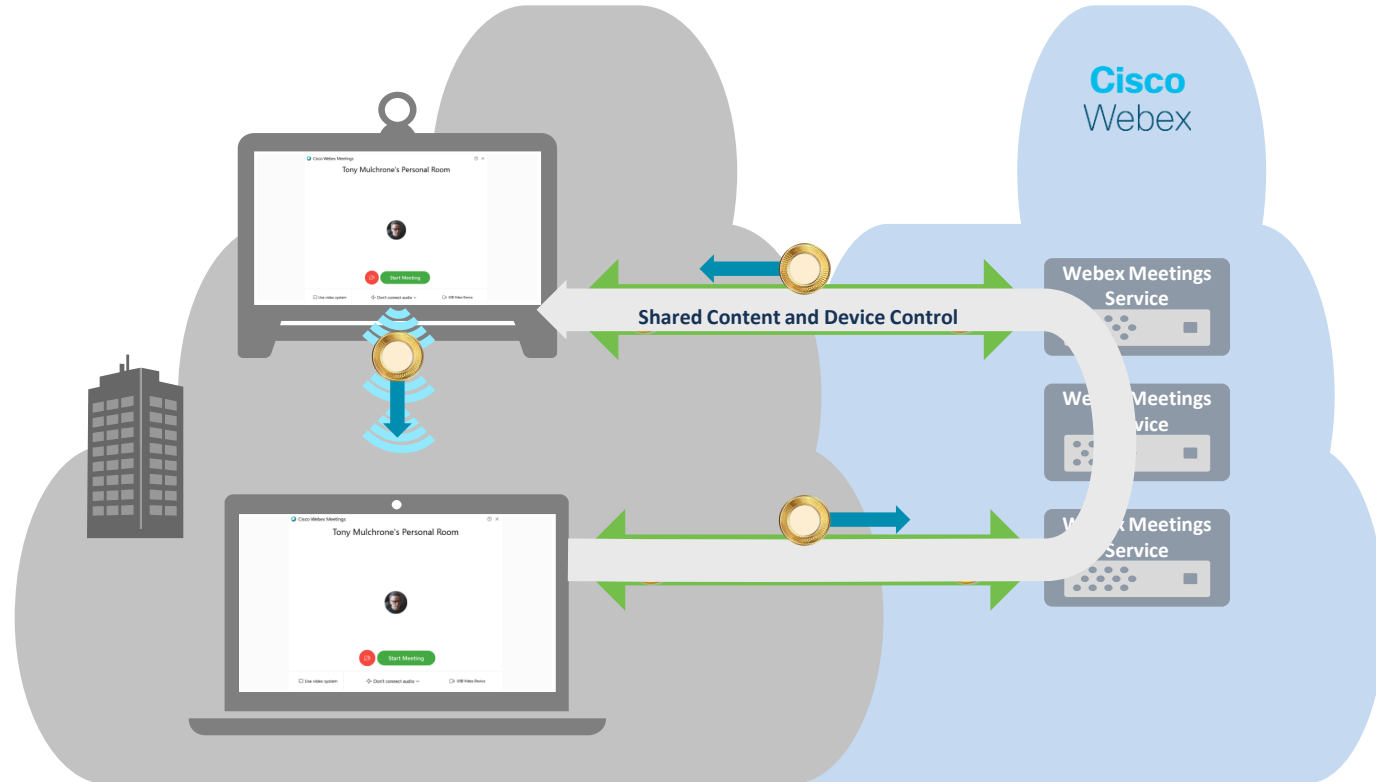
A Webex Meetings app within range of the ultrasound signal can use the received token to pair with Webex device, by sending the token to the Webex cloud service.



Webex Meetings Apps and Devices – Content sharing and device control

Once the paired via the Webex cloud, the Webex Meetings app can use the Webex device to connect to the meeting and to share content.

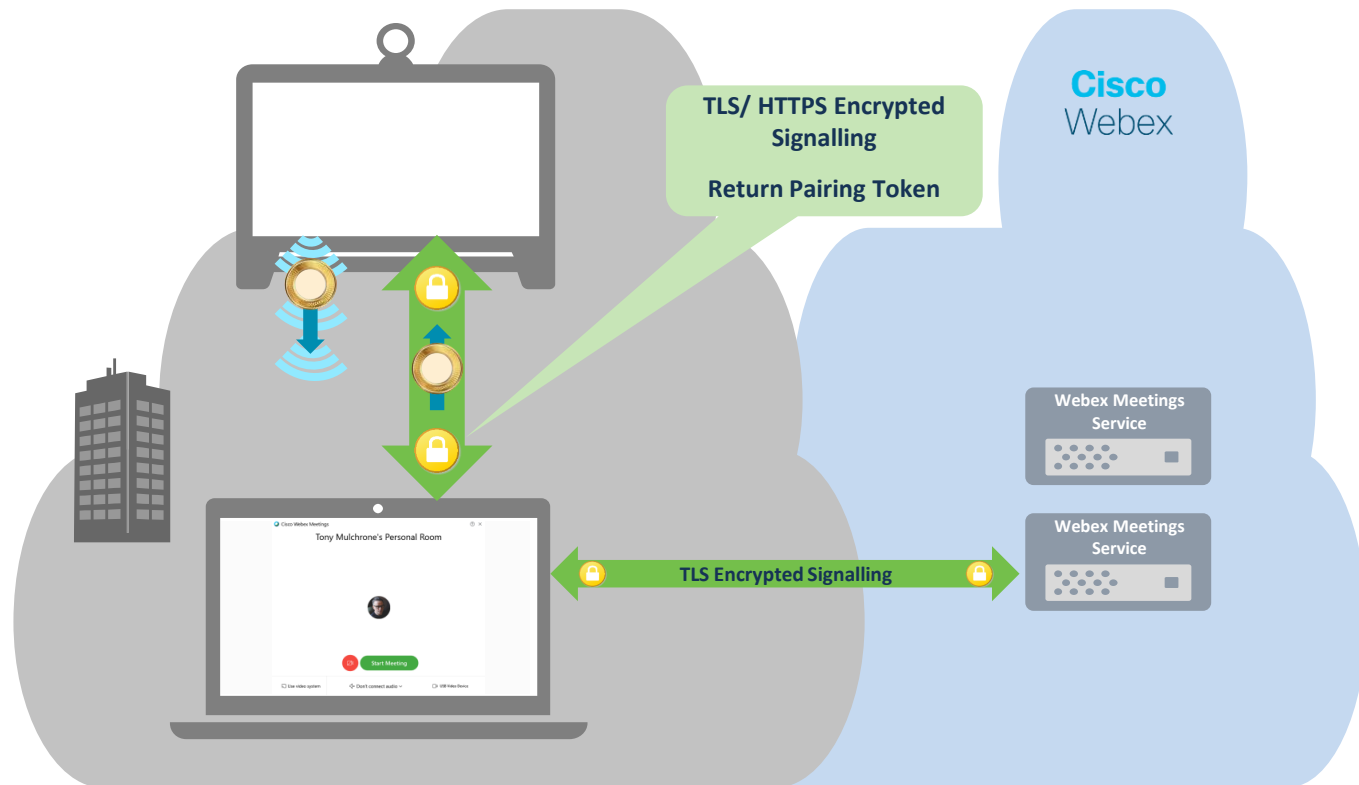
Both the app and device use their existing TLS connections to the Webex cloud, to exchange call control signalling and shared content.



Webex Meetings App and On Premises devices Proximity – Device detection and pairing

Unified CM registered video devices also use ultrasonic signalling for discovery and tokens for proximity pairing with Webex Meetings apps.

The Webex Meetings app and video device use a directly established HTTPS connection to exchange call control signalling and shared content.

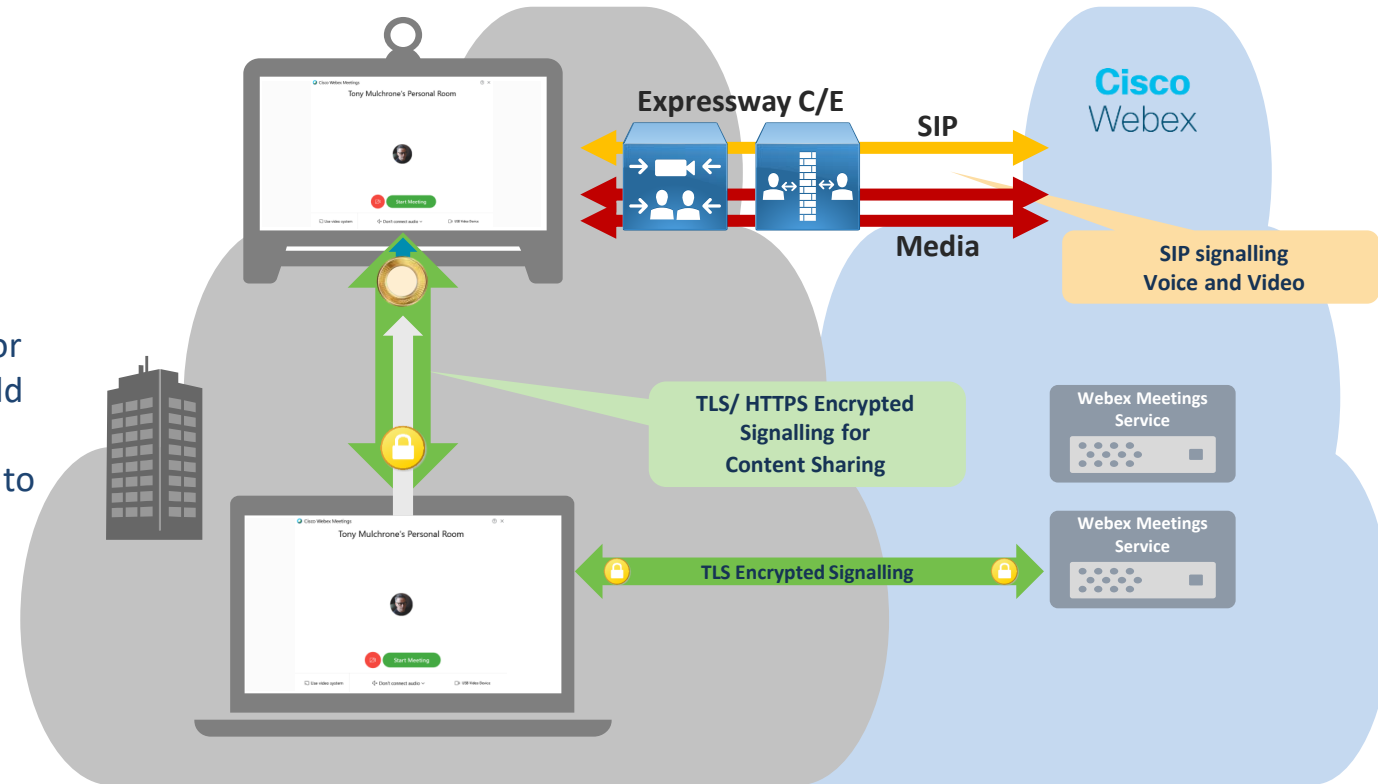


Webex Meetings Apps and On Premises Devices – Content sharing and device control

When connecting to an on-premises device, the content shared between the Webex Meetings app and device is always encrypted (HTTPS).

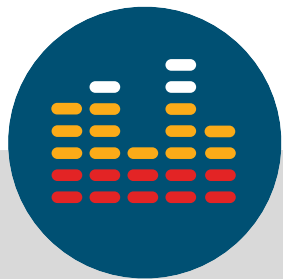
However, we don't enforce device certificate verification for the HTTPS session, as this would prevent pairing with guest devices and would be complex to deploy and maintain.

Device discovery can be disabled in Webex Meetings App preferences



Cognitive Collaboration for Webex Meetings

AI and Machine Learning in collaborative environments



Audio & Speech Technologies

Noise Detection

Speech Recognition

Meeting Transcription



Multi-modal Bots & Assistants

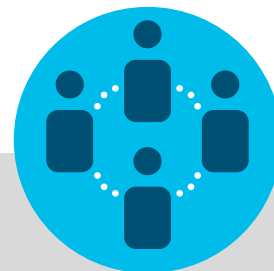
Collaboration Assistants

Care Assistants



Computer Vision

Face, Gesture and Object Recognition



Relationship Intelligence

People Profiles

Company Information

Cisco's Cognitive Collaboration Data Privacy Principles

- Don't retain data if you don't have to
- If you do, keep it for the shortest possible time
- Be transparent about data usage
- Provide Deletion Controls
- Empower end users
- **Data Handling and Privacy for Cognitive Collaboration White Paper**
- <https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html>

The screenshot displays the Cisco Webex Control Hub interface. On the left, a sidebar menu includes 'Overview', 'Users', 'Places', 'Services', and 'Devices'. The main content area is titled 'Face Recognition' and contains a 'Settings' section. The 'Settings' section has a toggle for 'Face Recognition' which is currently 'On'. Below the toggle, it states 'Status: On - 0/22 users have enrolled' and provides a link to 'Learn more about Face Recognition Name Labels'. A blue button labeled 'Invite users' is also present. Below the settings, there is a section titled 'Face Recognition & Your Privacy'. This section explains that Cisco's face recognition technology is designed with privacy in mind, ensuring compliance with privacy obligations. It details how the system uses a mathematical representation of a user's face to generate a name label. A user's photo is shown with a name label 'Giacomo' next to it. Below the photo, there is a 'Take a photo' button. The bottom of the screenshot shows a 'Show your name label' section with a toggle for 'Show your name label' which is currently 'On'. Below this, there is a 'Take a new photo' section with a 'Start' button. At the bottom, there is a 'Delete your data' section with a 'Delete' button.

Cisco Webex Control Hub

- Overview
- Users
- Places
- Services
- Devices

Face Recognition

Using camera data to provide a smarter meeting experience.

Recommended to provide the best experience for remote participants. When the camera of certain devices recognizes someone's face, the video displays the person's name below their face. [Learn more about Face Recognition Name Labels](#)

Status: On - 0/22 users have enrolled

[Invite users](#)

Face Recognition & Your Privacy

Cisco's face recognition technology is designed with privacy in mind to ensure we comply with our privacy obligations throughout the world. It allows you to take advantage of the name label feature in video meetings that you join from a Cisco room device. The feature displays your name next to your face so that you can be easily identified by other attendees.

When you enable the feature for the first time, you will be prompted to give Cisco permission to capture a photo of your face, which Cisco uses to generate a mathematical representation of your face. In order to ensure a higher rate of accuracy including are included labels.

You have mathematical face recognition data. For

to and the d, your cloud. You time by noto or gnition nt.

Take a photo

Make sure your face is fully visible.

[Take photo](#)

Show your name label

When this feature is enabled, meeting attendees on the other end of a video call can see your name next to you.

Take a new photo

A recent photo of you improves how well the system recognized you.

[Start](#)

Delete your data

You can delete your photos and associated face recognition data anytime. Once deleted, Cisco will not be able to recognize your face to personalize your experience.

[Delete](#)

Webex Meetings

Administrative Security Features for Meetings

Webex Meetings : Administrative Security Features

Webex Sites

- Multiple sites supported e.g.
- company-a-external.webex.com
- company-a-internal.webex.com

Webex Meetings Site Level Controls

- Session (Meeting) Types

Scheduled Meetings

- Recommended configuration for secure scheduled meetings
- Webex Site Security Controls
- End User Security Controls

Personal Meeting Rooms (PMRs)

- Recommended configuration for secure personal meetings
- Webex Site Security Controls
- End User Security Controls

Webex Meetings - Site Level Security Controls : Session Types

Configuration > Common Site Settings > Session Types >

- A standard set of default meeting session types :
 - Standard Meeting (STD)
 - Pro Meeting (PRO)
 - Online Event (ONS)
 - Training Session (TRS)
 - End to End Encrypted Meetings (E2E) *(by request)
- An administrator can modify the meeting capabilities of these default meeting session types
- An administrator can also create additional custom meeting session types (PRO Session Example)
- Site Admin User settings allows an administrator to make these meeting session types available to individual users
- Users can select the meeting type they want to use when scheduling a meeting via their personal Webex page

Edit Custom Session Type

Session Code : PRO4


Session Name : PRO Session Example

Features	
<input checked="" type="checkbox"/>	Alert - sound
<input checked="" type="checkbox"/>	Application Sharing
<input checked="" type="checkbox"/>	Chat
<input checked="" type="checkbox"/>	Desktop Sharing
<input checked="" type="checkbox"/>	Meeting Transcript
<input checked="" type="checkbox"/>	Recording Network Based
<input type="checkbox"/>	Recording Client-Side
<input checked="" type="checkbox"/>	Whiteboard
<input checked="" type="checkbox"/>	Annotation Tools
<input checked="" type="checkbox"/>	Notes
<input checked="" type="checkbox"/>	Polling
<input type="checkbox"/>	End-to-End-Encryption
<input checked="" type="checkbox"/>	Participant can grab presenter role
<input checked="" type="checkbox"/>	Desktop Sharing Remote Control
<input type="checkbox"/>

Webex Scheduled Meetings

Ephemeral Meetings
Password Protected Meetings
Unique Meeting URLs
Meeting Lock
Meeting Lobby
User Webex page scheduling
Calendar based scheduling
Encrypted chat
Encrypted media

Webex Meeting Host Security Controls : Scheduled Meeting Rooms



- Home
- Meetings
- Recordings
- Preferences
- Insights
- Support
- Downloads
- Feedback

Meeting Type :
(available meeting types set by site admin)

Meeting Topic (mandatory)

Meeting Password (mandatory and automatically generated)
Password can be changed by meeting host - password complexity set by site admin

Audio Connection Types
Webex Audio : Webex Apps, Webex Devices, SIP Devices, PSTN
VoIP Only : Webex Apps, Webex Devices, SIP Devices

Require Account : ☐ require attendees to have an account on this site in order to join this meeting

Exclude Password : Exclude password from email invitation

Webex Meetings Pro meeting ^

Webex Meetings Pro meeting

Webex Meetings Recording client-side

Webex Meetings Standard meeting

<https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts>

Webex Scheduled Meeting Rooms

Most commonly used Site Admin security settings

All Webex Scheduled Meetings have a meeting password
Enforce Meeting passwords for all participants (internal and external)

Webex Meetings Apps

Meeting password is embedded in the meeting join request from Webex Meetings Apps

- ✓ **PSTN meeting participants**
Enforce meeting password when joining by phone
(When checked, attendees must enter the numeric meeting password)
- ✓ **Video system meeting participants**
Enforce meeting password when joining from video systems
(When checked, attendees must enter the numeric meeting password)
- ✓ All meetings must be unlisted
- ✓ Display Caller ID for dial-in users when available

<https://help.webex.com/en-us/ov50hy/Cisco-Webex-Best-Practices-for-Secure-Meetings-Control-Hub>

Webex Scheduled Meeting Rooms

Site Admin security settings for secure internal meetings

All Webex scheduled meetings must have meeting password
Enforce Meeting passwords for all participants

Require Account : ☒ Require attendees to have an account on this site in order to join this meeting
This is a host setting for individual scheduled meetings

Webex Meetings Apps

Meeting password is embedded in the meeting join request from Webex Meetings Apps

PSTN meeting participants

- ☒ Require users to have an account when joining by phone (*Enforced when “Require Account” set*)
- ☒ Enforce meeting password when joining by phone (Attendees must enter numeric meeting password)

Video system meeting participants

- ☒ Enforce meeting password when joining from video systems (Mandatory numeric meeting password)
When sign-in is required to join meeting, video conferencing systems will be: Blocked ☐ Allowed ☒
- ☒ All meetings must be unlisted
- ☒ Display Caller ID for dial-in users when available

Webex Personal Meeting Rooms (PMRs)

- Persisted Meeting Rooms
- Host Activated Meetings
- Meeting Lock
- Meeting Lobby
- Start PMR from User's Webex page
- Use PMR for calendared meetings
- Encrypted chat
- Encrypted media

Webex Meetings – Meeting Host Security Controls : Personal Meeting Rooms



- Home
- Meetings
- Recordings
- Preferences
- Insights
- Support
- Downloads
- Feedback

Personal Room name : User defined

Personal Room link : <https://example.webex.com/meet/tmulchro>

Site admin can allow users to change the room URL (e.g. tmulchro → 12568901)

Host PIN : XXXXXX

The host PIN is used to start a personal room meeting, if the host is calling in via a PSTN, or Video endpoint. In general, the meeting host will also require access via the Webex App to admit users from the lobby and to control users in the meeting

Automatic Lock :

☒ Automatically lock my room m 0 tes after meeting starts so people can't enter until I admit them

Site Admin – User setting controls :

- User cannot change default setting set by site admin
- User allowed to change default setting set by site admin

<https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts>

Ways to use Webex Personal Meeting Rooms – Site Admin : Most secure deployment model

Configuring PMRs that allow internal users only

☒ **No one can enter a room or lobby without signing in**

☐ Allow host to start Personal Room meetings from phone

☒ Require users to have an account when joining by phone

When sign-in is required to join meeting, video conferencing systems will be: Blocked ☐ Allowed ☒

☒ Site Admin should Automatically lock Personal Rooms min s after meeting starts

☒ Do not allow hosts to change their Preferences > My Personal Room > Automatic lock setting

Host can unlock room to allow participants to join and then re-lock the room

☐ Allow hosts to change their Personal Room URLs

☒ Display Caller ID for dial-in users when available

<https://help.webex.com/en-us/ov50hy/Cisco-Webex-Best-Practices-for-Secure-Meetings-Control-Hub>

Ways to use Webex Personal Meeting Rooms – Site Admin: Secure but, accessible deployment model

Configuring PMRs that allow internal users and external participants

- ☒ Signed-in attendees can enter an unlocked room, but unauthenticated attendees must wait in the lobby until the host manually admits them
- ☐ Allow host to start Personal Room meetings from phone
- ☒ Site Admin should Automatically lock Personal Rooms min s after meeting starts
- ☒ Do not allow hosts to change their Preferences > My Personal Room > Automatic lock setting
Host can unlock room to allow participants to join and then re-lock the room
- ☐ Allow hosts to change their Personal Room URLs
- ☒ Display Caller ID for dial-in users when available

<https://help.webex.com/en-us/ov50hy/Cisco-Webex-Best-Practices-for-Secure-Meetings-Control-Hub>

Personal Meeting Rooms : Site Level Security Controls

Common Site Settings > Options

Security settings that can be applied to all PMR meetings

- ☒ Enable Personal Room (When enabled, you can turn this on or off for individual users)
- ☐ Allow host to start Personal Room meetings from phone Host PIN length
- ☐ Allow hosts to change their Personal Room URLs
- ☐ Anyone can enter an unlocked room
- ☒ Signed-in attendees can enter an unlocked room, but unauthenticated attendees must wait in the lobby until the host manually admits them
- ☐ No one can enter a room or lobby without signing in
- ☒ Automatically lock Personal Rooms min minutes after meeting starts for any users who have not defined their Preferences > My Personal Room > Automatic lock setting (options 0/5/10/15/20 mins)
 - ☒ Do not allow hosts to change their Preferences > My Personal Room > Automatic lock setting
- When sign-in is required to join meeting, video conferencing systems will be: Blocked ☐ Allowed ☒
- ☒ Display Caller ID for dial-in users when available
- ☒ Allow Web access AI ☒ iOS access AI ☒ Android access
- ☐ Require users to have an account when joining by phone

Online Documents :

Webex Meetings Security
and Privacy

Webex Meetings Security – Documentation

Webex Meetings Security White Paper

<https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf>

Webex Meetings Privacy Data sheet

<https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf>

Cisco Master Data Protection Agreement

<https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf>

Data Handling and Privacy for Cognitive Collaboration White Paper

<https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html>

Network Requirements for Webex Meetings Services

<https://help.webex.com/en-us/WBX264/How-Do-I-Allow-Webex-Meetings-Traffic-on-My-Network>

How End to End Encryption works

<https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do>

Complete your online session evaluation

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live socks.
- All surveys can be taken in the Cisco Live Mobile App or by logging in to the Session Catalog on ciscolive.com/us.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com/us.

Thank you



Possibilities

#CiscoLive