The bridge to possible

Securing Webex Meetings and avoiding meeting fraud

Privacy, Confidentiality and Security options for meetings in a virtual world

Tony Mulchrone
Principal Product Manager
Webex Security

cisco Live!

BRKCOL-2876

Cisco Webex App

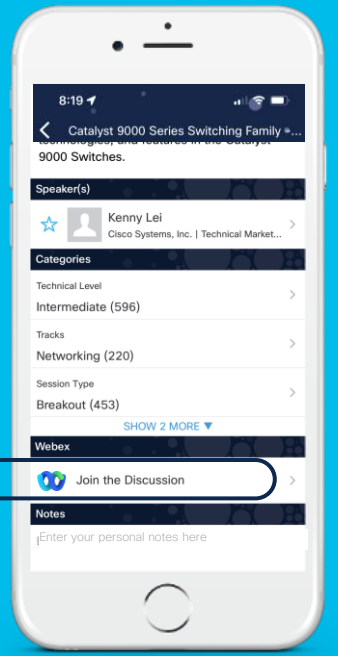
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

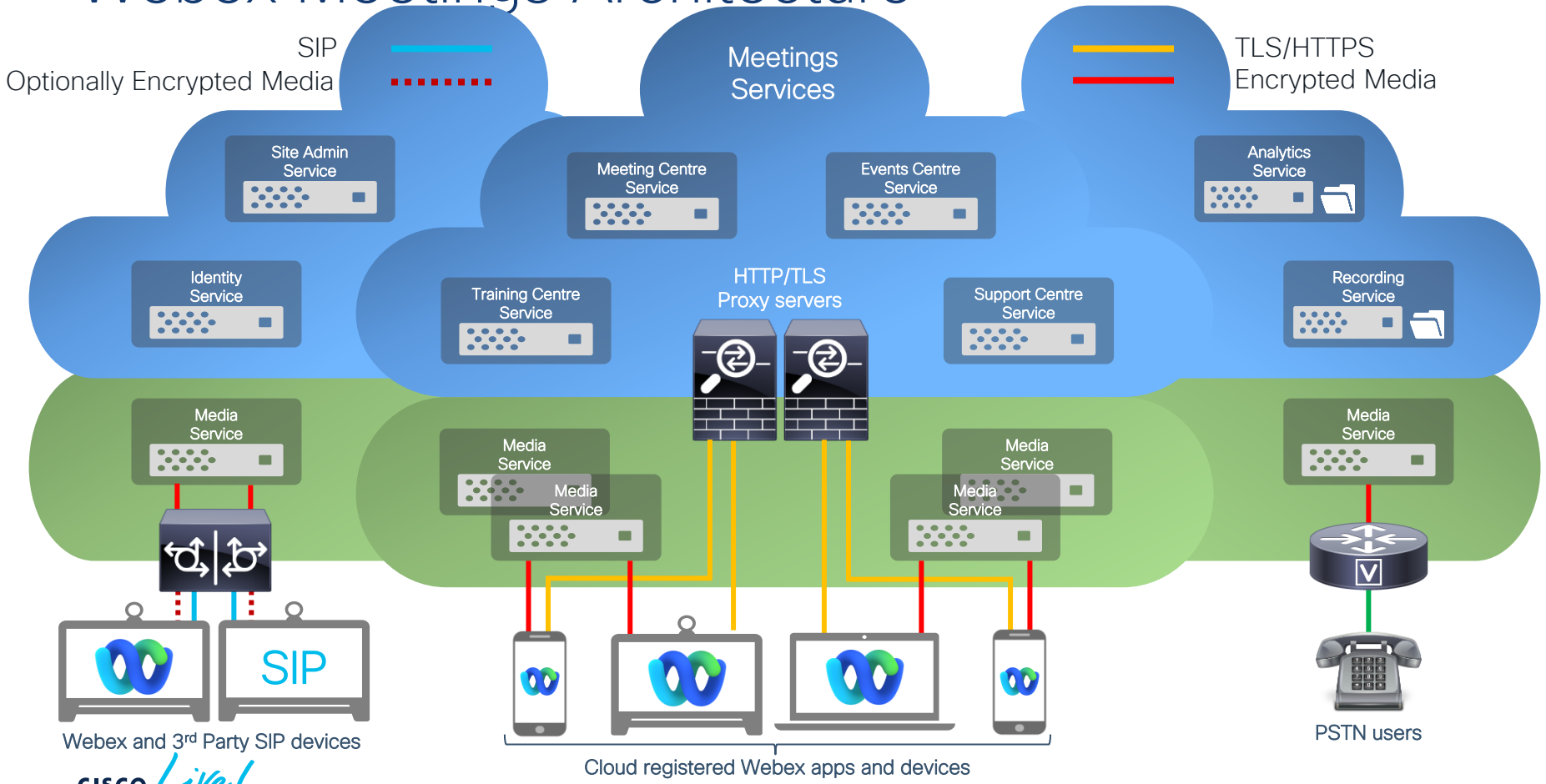
Webex spaces will be moderated until February 24, 2023.



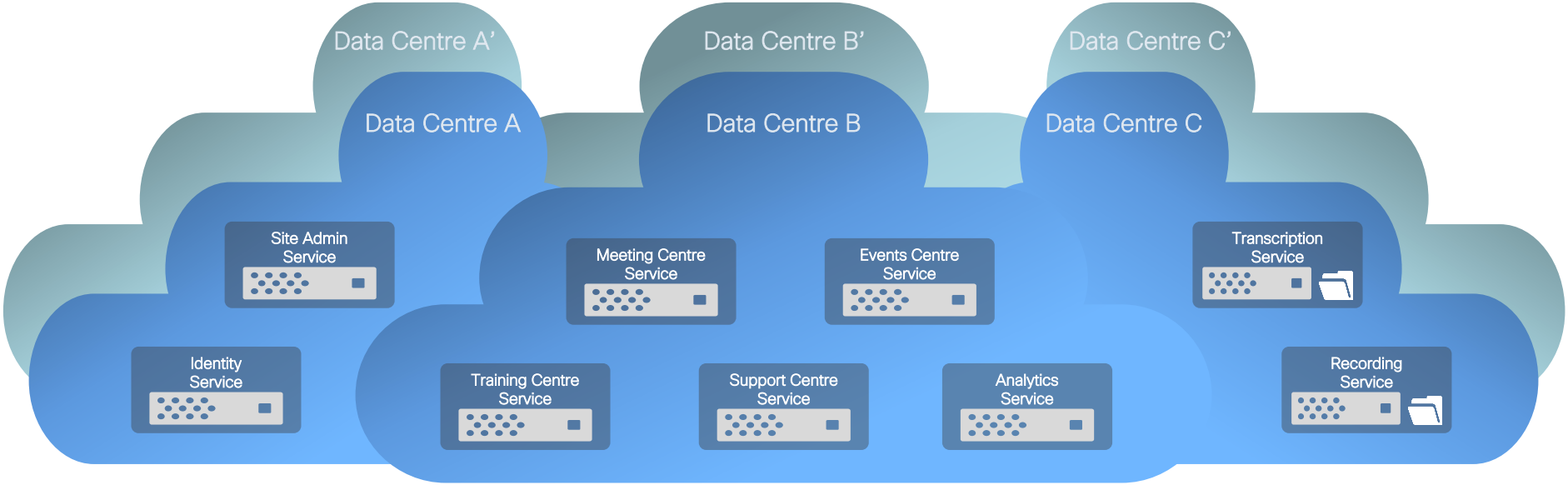
Agenda

- Introduction
- Secure Webex platform
- Secure Webex Meeting Types : Standard, E2EE, Private
- Scheduled Webex Meetings and Webex Personal Rooms
- Securing Webex Meetings and avoiding meeting fraud
- Privacy features – Deleting meeting metadata

Webex Meetings Architecture



Webex Meetings Regions and Redundancy



Webex Services for Webex Meetings/ Events/ Training/ Support, Identity, Recording are regionalized and replicated across independent data centres.

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

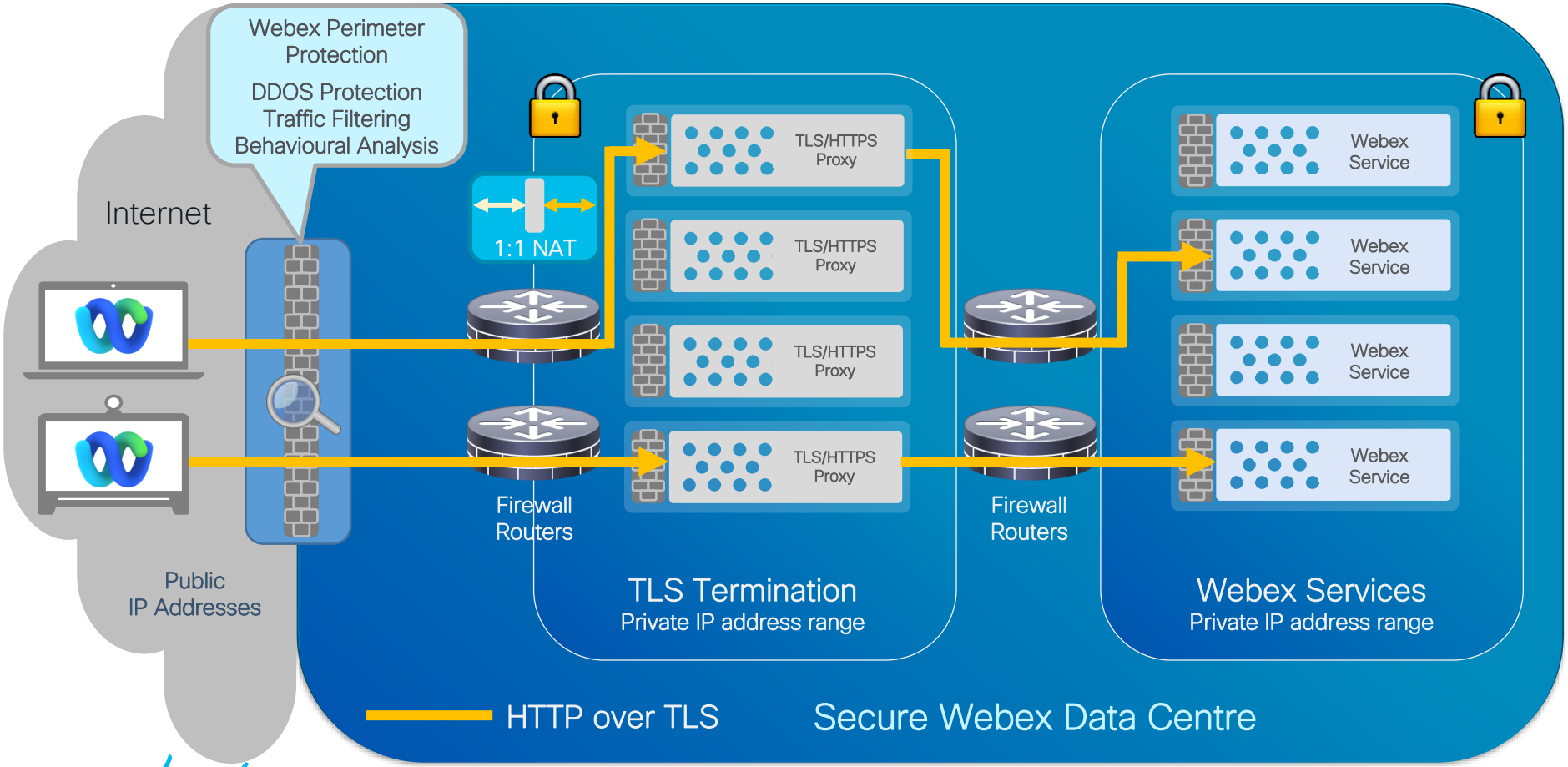
Webex Meetings regions: EU/ UK/ US/ Canada/ APAC/ Australia

Webex Meetings : Secure Platform

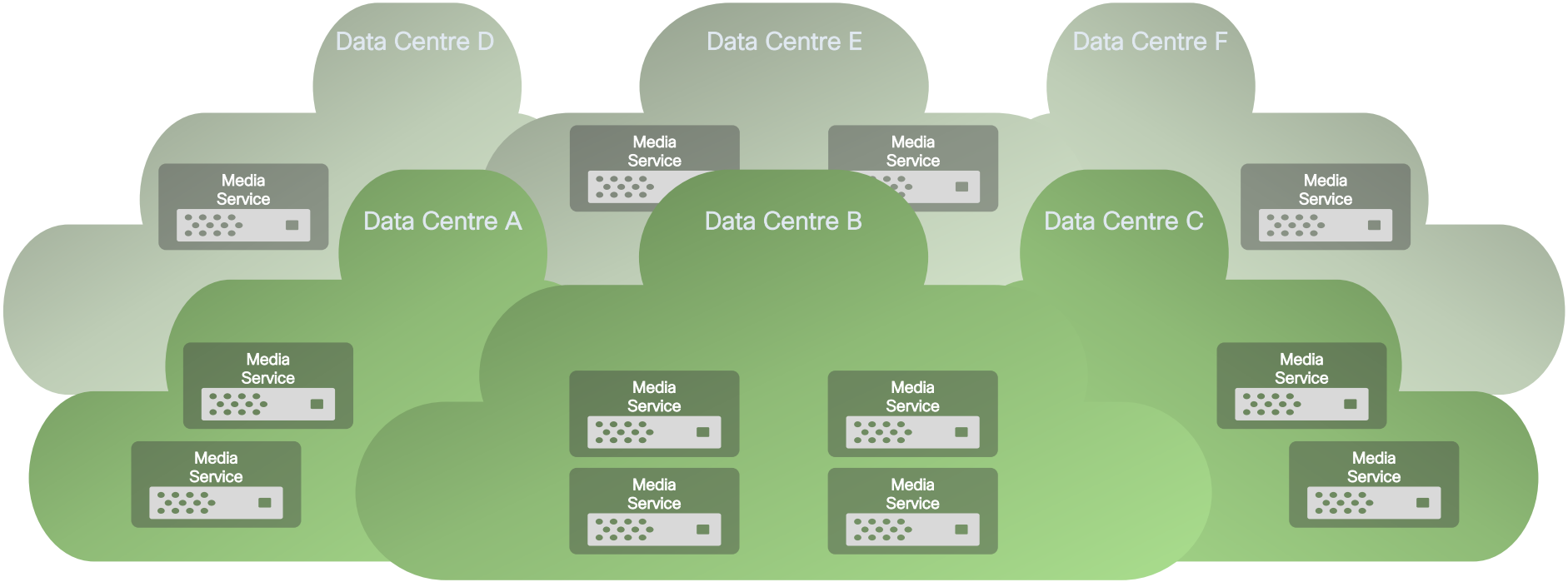
- TLS signalling
- Encrypted Media

Network Requirements for Webex Meetings and Messaging services
https://help.webex.com/en-us/WBX000028782

Webex encrypted HTTP signaling – TLS/HTTPS traffic

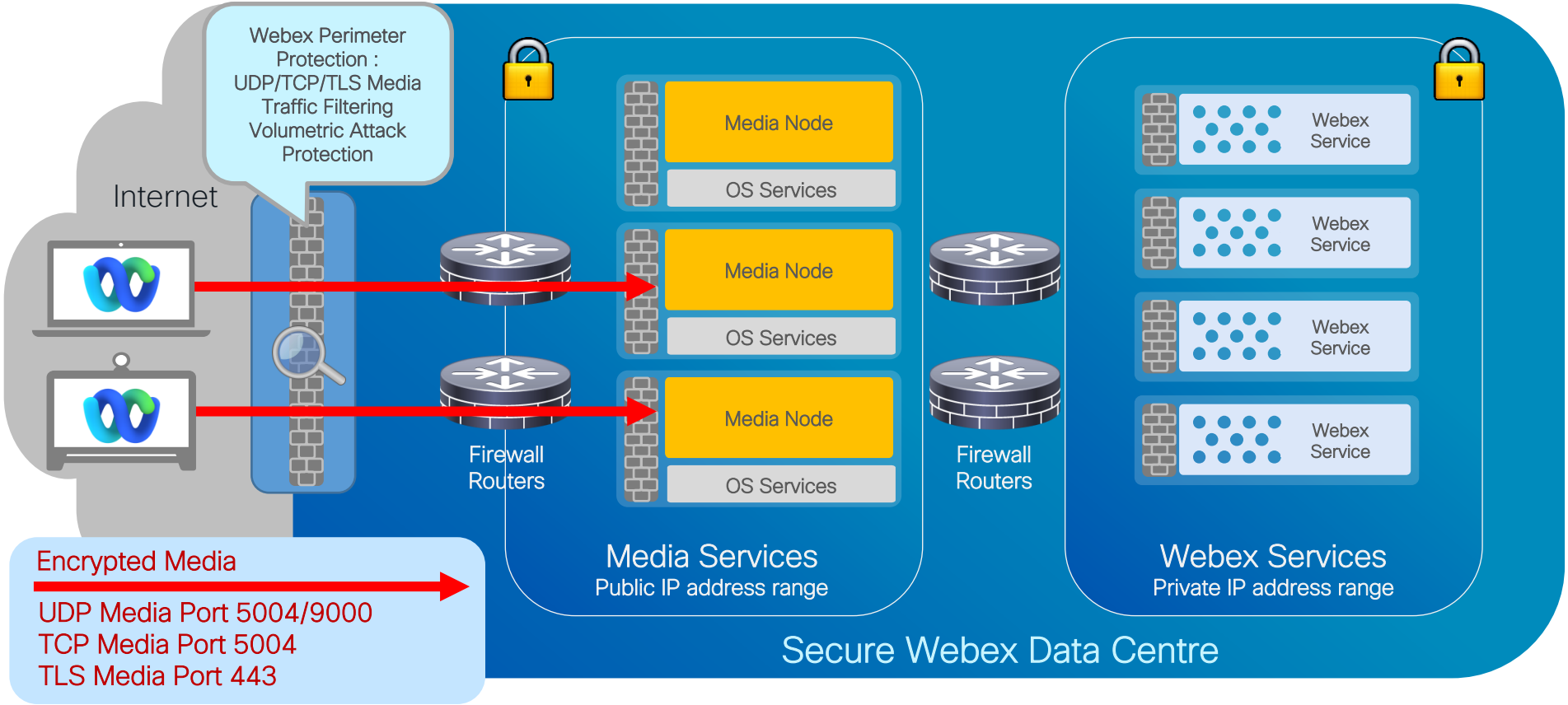


Webex Media Services



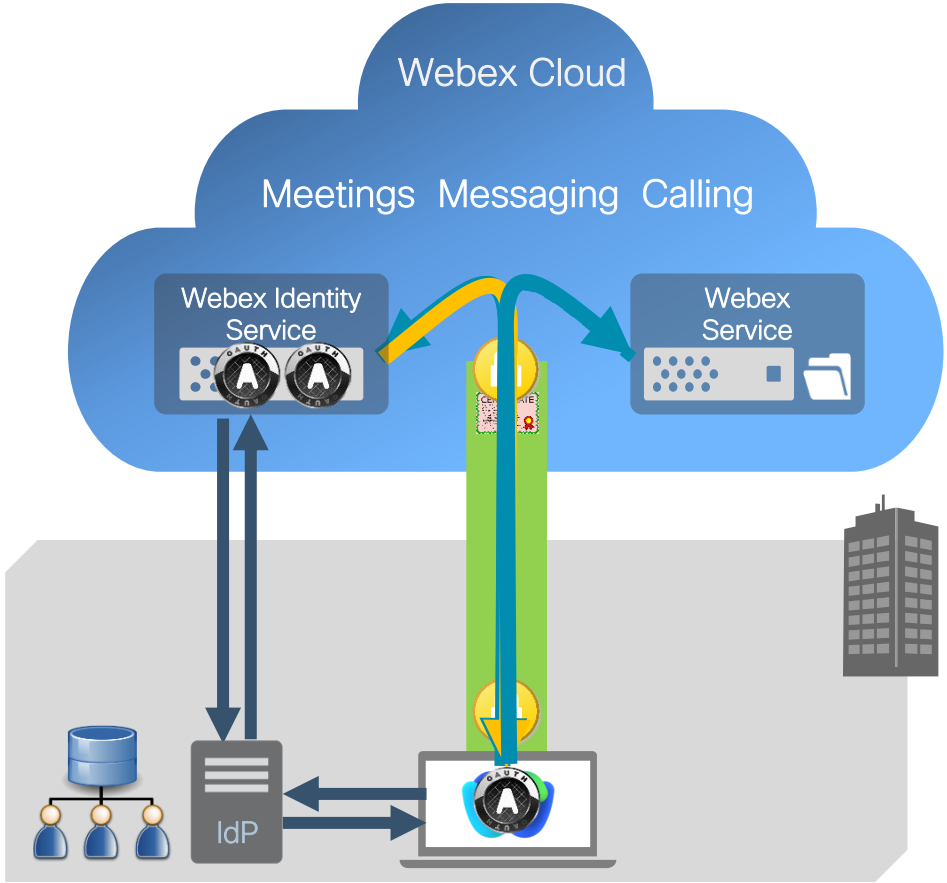
Webex Media services are globally distributed across multiple data centres
Media Server clusters in each data centre provide local and geographic redundancy
Media servers support voice, video and content sharing
All media is encrypted

Webex Media Services : Encrypted Media



Webex Media Encryption cipher : AEAD-AES-256-GCM

Webex app – app download and cloud registration



1) Customer downloads and installs the Webex app
2) Webex app establishes a secure TLS connection with the Webex Cloud
3) Webex Identity Service prompts User for an e-mail ID
4) User Authenticated by Webex Identity Service, or Enterprise IdP (SSO)
5) OAuth Access and Refresh Tokens created and sent to Webex app
   - The Access Token contain details of the Webex resources the User is authorised to access
5) Webex app presents its Access Token to register with Webex Services over a secure channel

Webex Room Devices – Onboarding and Registration

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

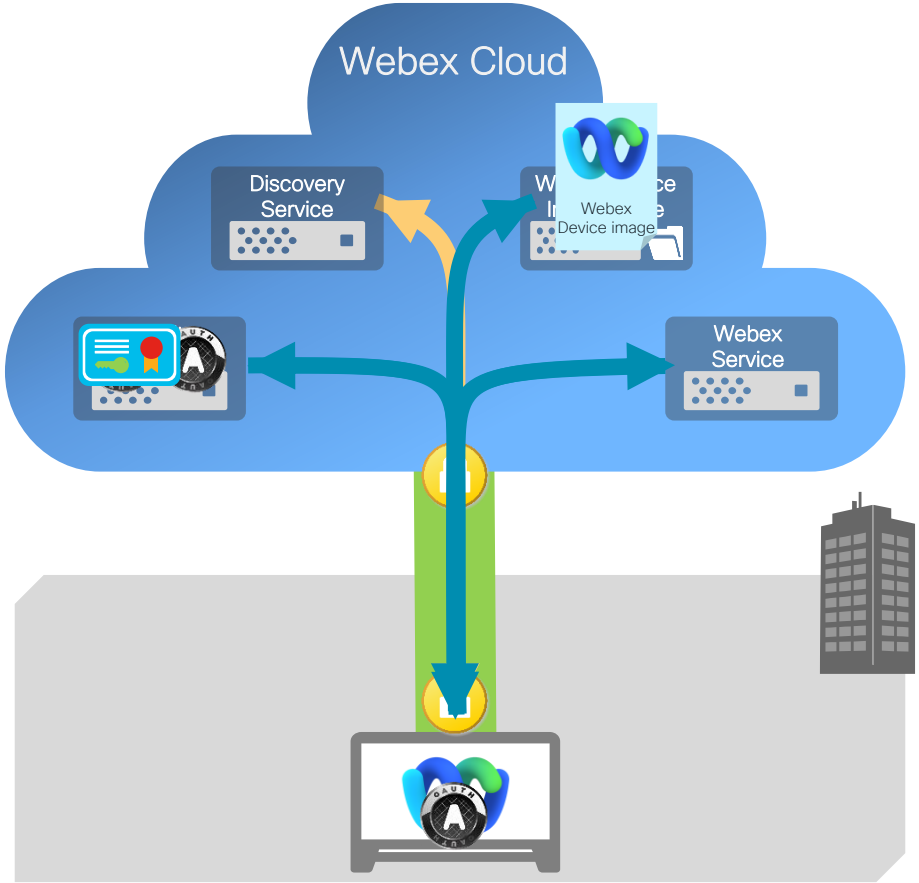
Webex Control Hub administrator generates device activation code for the device

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 Certificate Trust List* to the device over direct PAKE SRP secured channel

Device checks current software version. If upgrade required, a signed image is sent to the device. Signed image verified and installed

Device registers to Webex Services



* Can include Enterprise CA Certs for TLS Proxy inspection

1234567890123456

Webex Meetings
Secure Meeting Types :

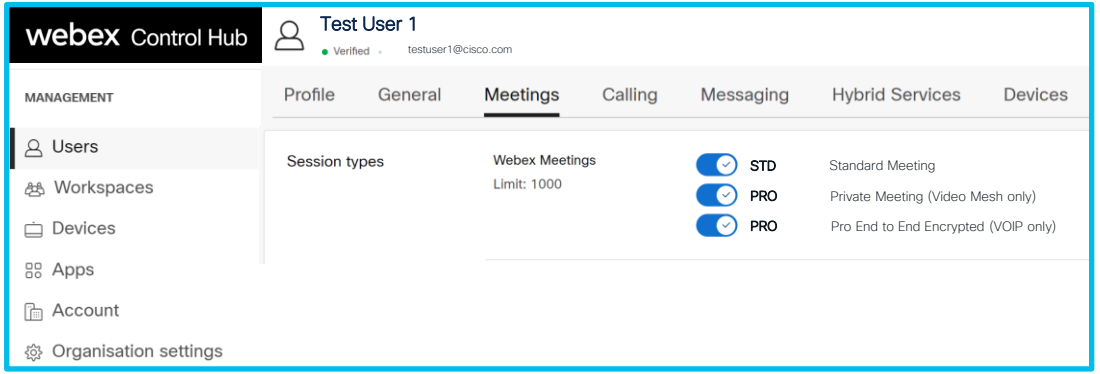
- Standard Meetings
- End to End Encrypted Meetings
- Private Meetings

Assigning and Selecting Webex Meeting Types

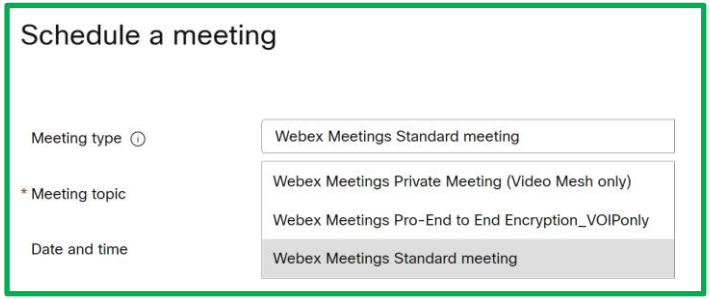
Webex Control Hub (and Site Admin)
Administrator can assign various default meeting session types to users

Administrator can also create new bespoke meeting session types and assign these to users

All available session types can be enabled/ disabled per user



Meeting Host/ Scheduler
When scheduling a meeting via the user's webpage
The user will see the selection of meeting session types assigned to them by the administrator
User selects their preferred meeting session type for the meeting



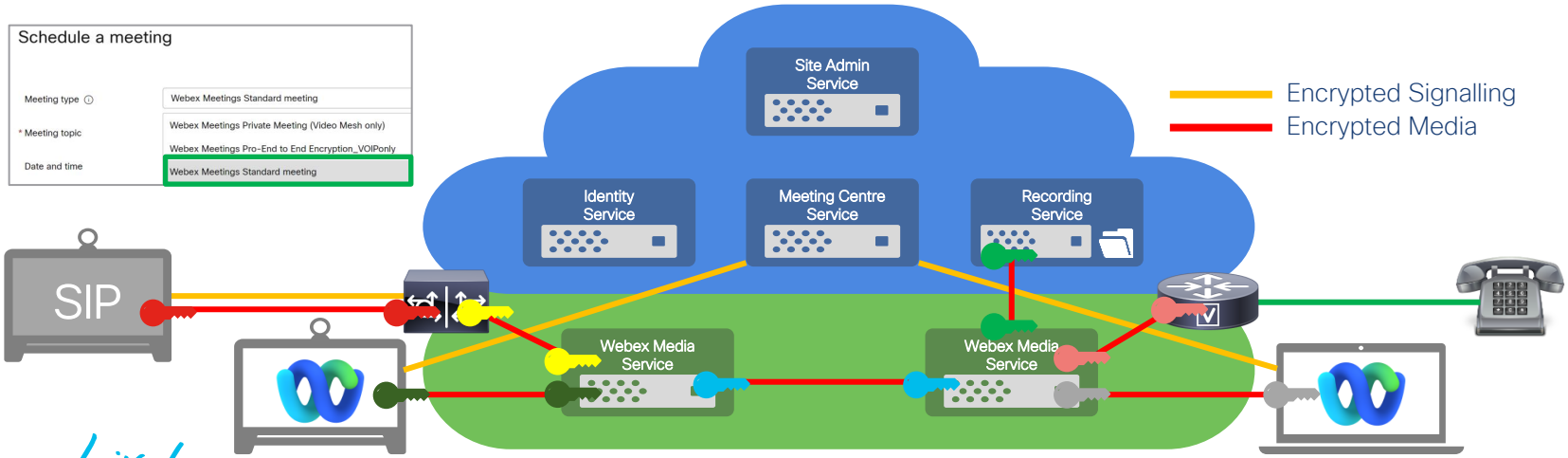
Encryption for standard Webex Meetings

With standard Webex Meetings, all signalling and media in the Webex cloud is encrypted
Webex apps and devices use encrypted signalling and encrypted media
SIP devices can encrypt signalling and media, PSTN audio is encrypted by the Webex cloud

With standard Webex Meetings, the cloud needs to access to encryption keys to decrypt SRTP media from SIP devices, PSTN gateways and for other services such as recording

Every vendor of cloud meeting services requires access to meeting encryption keys for SIP, H323, PSTN and other services

- Privacy & Confidentiality (Hop by Hop encryption)
- Accessibility (Anyone : Cloud, SIP, PSTN users)
- Features (All : Recording, Transcripts, Webex Assistant etc)

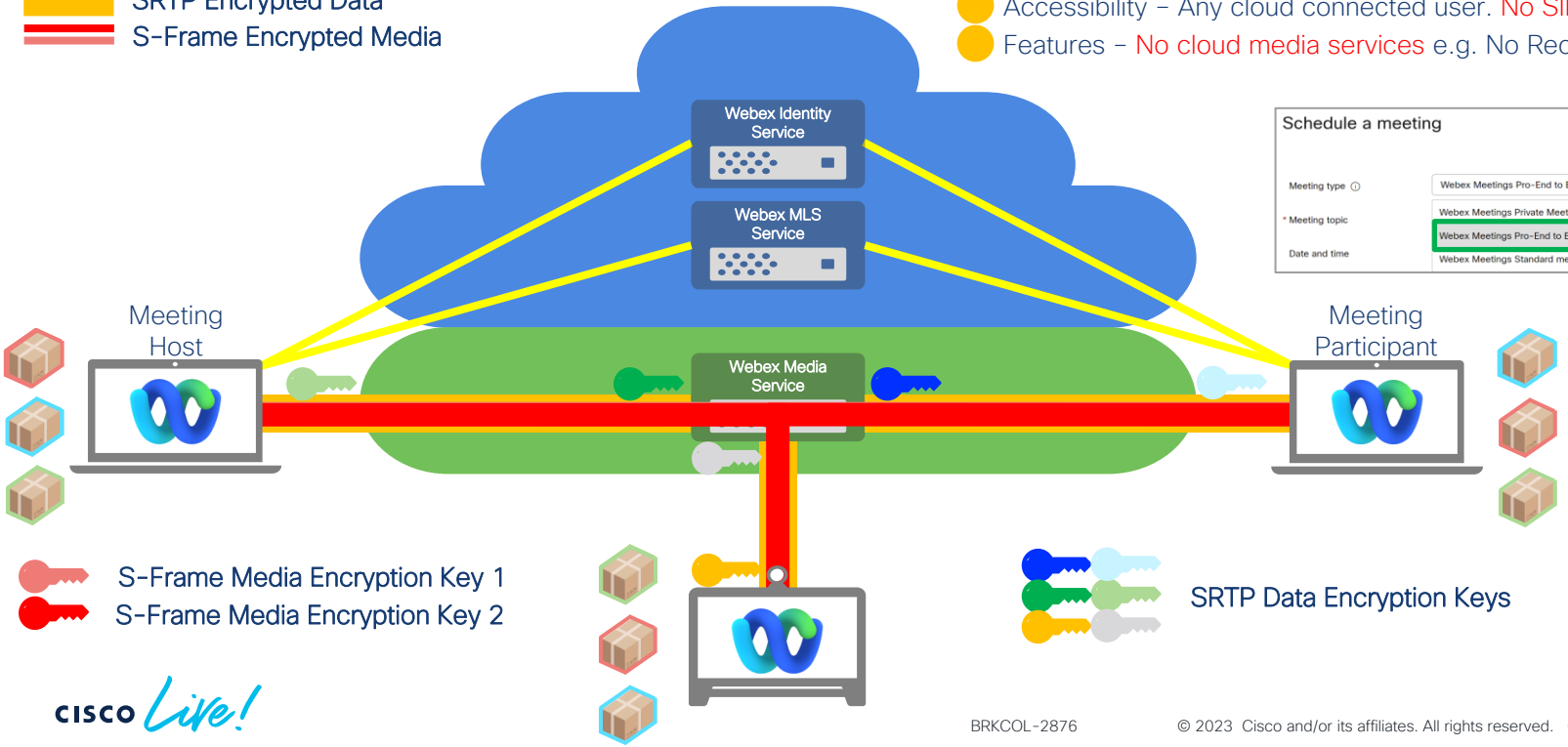


Webex Zero Trust End to End Encrypted Meetings

With Webex Zero Trust E2E encrypted Meetings, the Webex cloud does not have access your meeting encryption key
For details see https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

TLS/HTTPS
SRTP Encrypted Data
S-Frame Encrypted Media

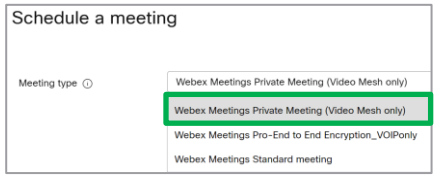
Privacy & Confidentiality (Cloud cannot decrypt media)
Accessibility – Any cloud connected user. No SIP, No PSTN
Features – No cloud media services e.g. No Recording, WXA etc



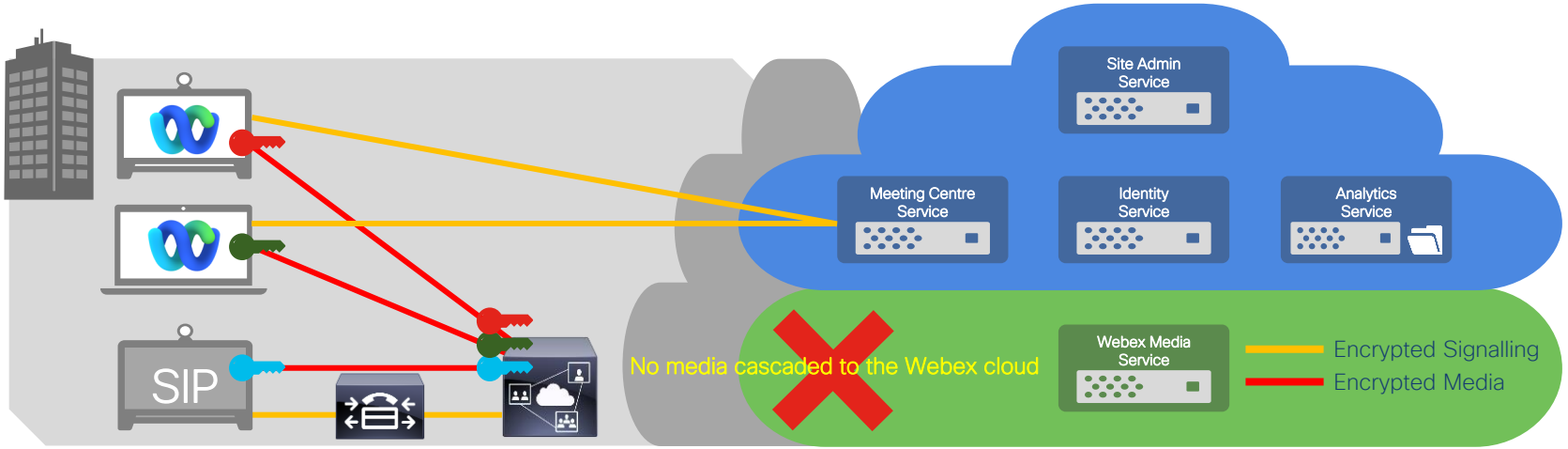
Encryption for Private Webex Meetings

- All media is switched in the on premises Webex Video Mesh Node
- No media cascades to the Webex cloud
- Cloud registered Webex apps and devices always use encrypted signalling and encrypted media
- On Premise Webex and 3rd Party SIP apps and devices may use encrypted signalling and encrypted media

All apps and devices must have access to the Webex Video Mesh Node on premises



- Privacy & Confidentiality – Media kept on premises
- Accessibility – My org only : Cloud and SIP based users
- Features – No cloud media services



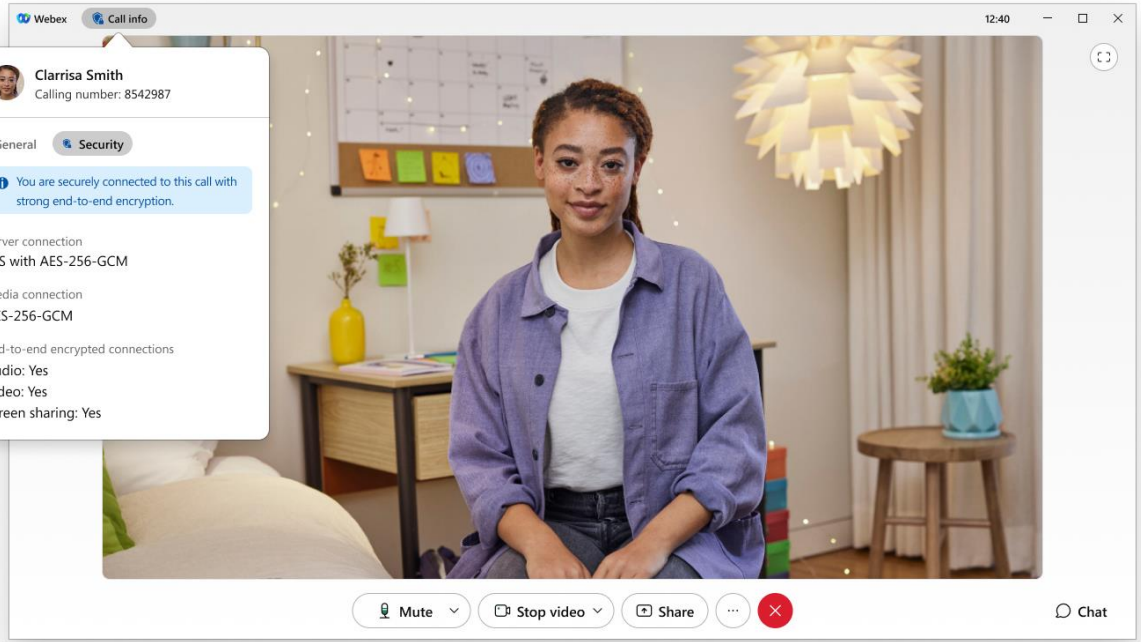
Video Mesh Node Private Meeting

Zero Trust Security for one-to-one calls

Coming soon

Modern, standards-based Zero Trust E2E Encryption for one-to-one calls with the Webex App

- Zero Trust End-to-End Encryption (E2EE) of Media
- Verified identity
- Standards-based, formally-verified cryptography (MLS)
- Webex App support
- Escalate Calls to E2EE at the push of a button



General Availability : Planned for Q2 CY2023

Webex Meetings :

Scheduled Meetings and Personal Room Meetings

Scheduled Webex Meetings

Most secure and preferred meeting type

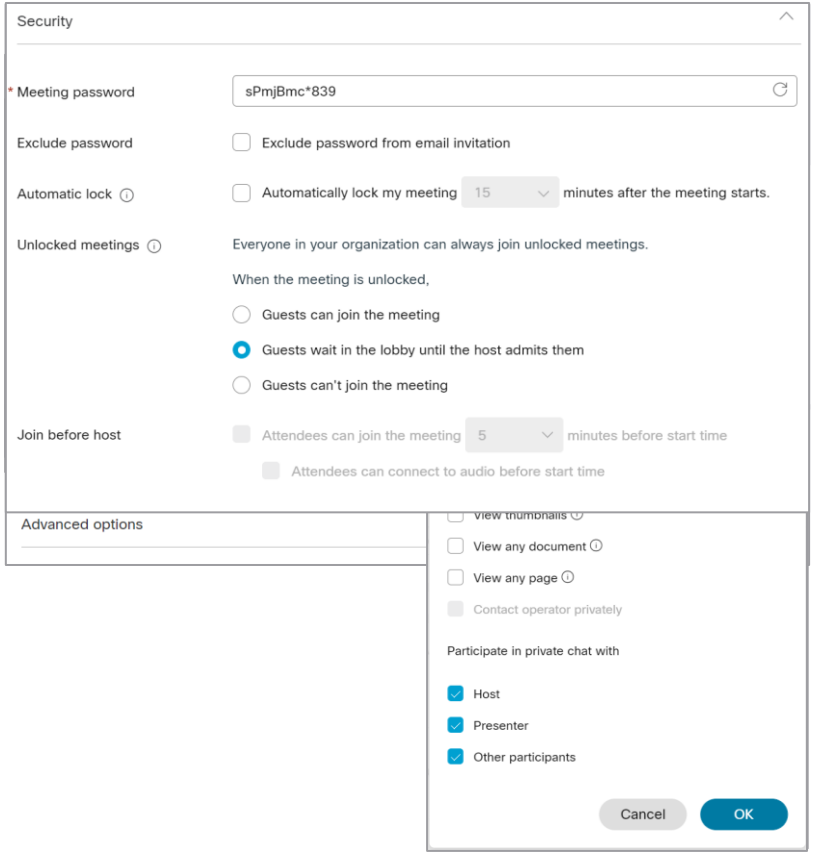
- Multiple meeting types available
- One time meeting or recurring

- Password protected
- Auto Lock feature
- Lobby Controls
- Join before Host controls

- Call In numbers
- Attendee mute controls

- Recording Controls
- Enable Breakout sessions
- Require invitees to register
- Simultaneous Interpretation

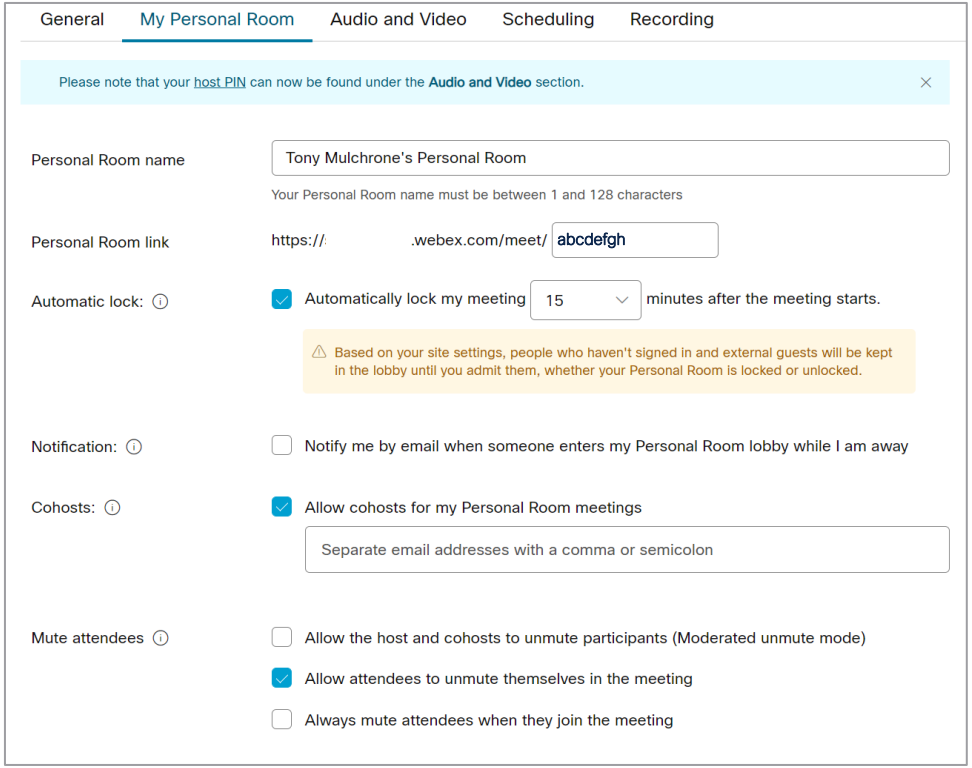
- Meeting Options
- Attendee Privileges



Webex Personal Room Meetings

A convenient meeting type, but recommended for meetings with trusted participants

- Personal Room Meetings
  - A persisted meeting
  - Always available
  - Activated by the host (or co-host)
- Limited security features :
  - Lobby (Site Admin controlled)
  - Lock (Site Admin/Host controlled)
  - CAPTCHA (Site Admin controlled)
- Mute attendee controls



Secure Meeting access : PSTN/ SIP/ Cloud devices

The richest meeting experience comes with the Webex app, but
Users can also join meetings from cloud registered Webex devices, SIP devices, Phones…

In Meeting Features	Security Features
Cloud registered Webex devices • Audio/ Video/ Desktop share • Meeting Roster, Reactions, • One Button to Push, Noise Reduction • Webex Assistant, Closed Captions • Recording etc	Cloud registered Webex device security Webex recognizes cloud registered devices and can apply security privileges such as Lobby bypass
SIP devices • Audio/ Video/ Desktop share PSTN/ IP Phones • Audio only	Security for SIP devices & Phone users DTMF entered – meeting number & numeric password Video system settings : Enforce numeric meeting password when joining Phone settings : Require users to sign in before joining meeting Enforce numeric meeting password when joining by phone

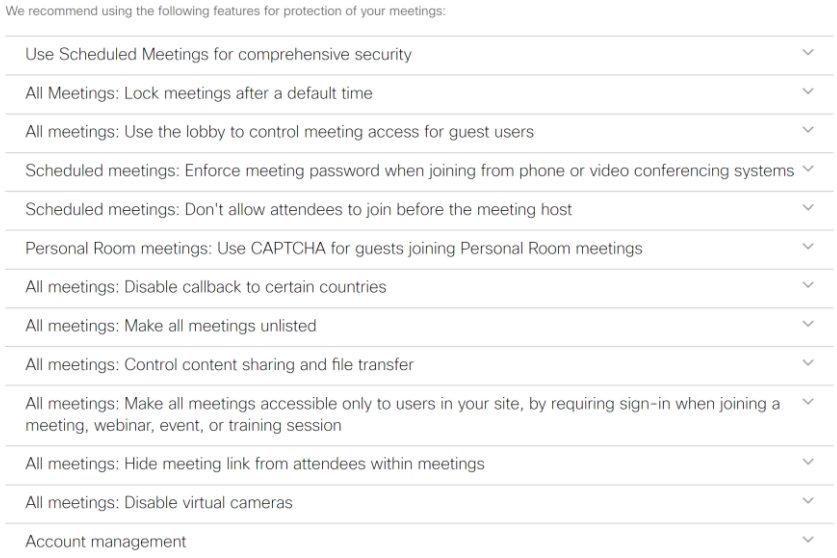
Administrator and Meeting Host - Security documents

Webex best practices for secure meetings: Control Hub

https://help.webex.com/en-us/article/ov50hy/Webex-best-practices-for-secure-meetings:-Control-Hub

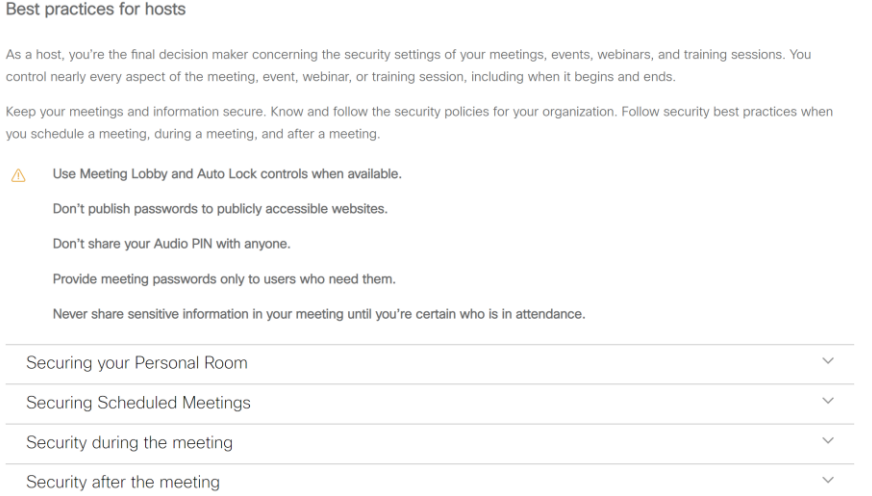
Webex best practices for secure meetings: Site Administration

https://help.webex.com/en-us/article/v5rgi1/Webex-best-practices-for-secure-meetings:-Site-Administration



Webex best practices for secure meetings: hosts

https://help.webex.com/en-us/article/8zi8tq/Webex-best-practices-for-secure-meetings:-hosts



Webex Meetings :

Webex Meeting Security Features

Deepfake and other exploits…

Avoiding fraud and unwanted attendees

Webex features for user screening & controlled access to meetings

Deepfake and online meetings

- Deepfake software is freely available today
- Deepfake exploits are usually sophisticated attacks or doctored pre-recorded video
- Instances of meetings with fraudulent users using deepfake are relatively small today, but there have been several significant cases

To avoid deepfake users in meetings…..

- The host need tools that allows them to check the validity of a user's identity
- The host needs to be able to vet individual users and eject unwanted users
- Participants need an indicator of the authenticity of each user

Webex has these tools…..


The Guardian
News website of the year

European MPs targeted by deepfake video calls imitating Russian opposition

Politicians from the UK, Latvia, Estonia and Lithuania tricked by fake meetings with opposition figures

The real Leonid Volkov, Russian opposition politician and close ally of Alexei Navalny, in March 2021. He said the deepfake of him used in the calls was 'virtually identical'. Photograph: Petras Malūkas/AFP/Getty Images

A series of senior European MPs have been approached in recent days by individuals who appear to be using deepfake filters to imitate Russian opposition figures during video calls.


The Guardian
News website of the year

European politicians duped into deepfake video calls with mayor of Kyiv

Person who sounds and looks like Vitali Klitschko has spoken with mayors of Berlin, Madrid and Vienna

Someone has been impersonating the mayor of Kyiv, Vitali Klitschko – the real one seen here. Photograph: Markus Schreiber/AP

The mayors of several European capitals have been duped into holding video calls with a deepfake of their counterpart in Kyiv, Vitali Klitschko.

Less sophisticated, but more common meeting fraud exploits

Meeting fraud is generally of two types :

1) PSTN Call Back Toll Fraud
   Unwanted users join meetings and initiate a call back to a premium rate number
   The organization hosting the meeting pays the bill for these premium rate calls

2) Eavesdroppers/ unwanted users
   At best, these attackers will disrupt your meeting
   At worst, unwanted access information that your organization considers confidential

The majority of meeting fraud today is perpetrated by unverified (guest) users

An unverified user is any user who does not have a Webex account, or has not signed in

Allowing unverified users to join your meetings, makes meetings easily accessible to any user
- This can be beneficial, when a required attendee does not have a Webex account (paid/ free)
- The downside is that an unverified user is exactly that… they can enter any username, and the meeting host cannot verify their identity until they are in the meeting

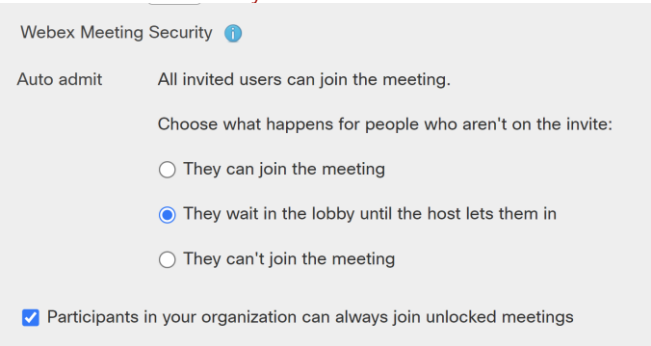
New Webex Meetings Security features

- Scheduled Meetings : Auto Admit feature
- Personal Meeting Rooms : New Lobby Controls
- Organization/ User Group/ User :
  - External Meeting Access Controls
  - Internal Meeting Access Controls
  - External Meeting Feature Controls
  - Internal Meeting Feature Controls
- Meeting Lobby/Roster/Video : Identity Labels
- Vetting Users in the Lobby – Move to breakout room

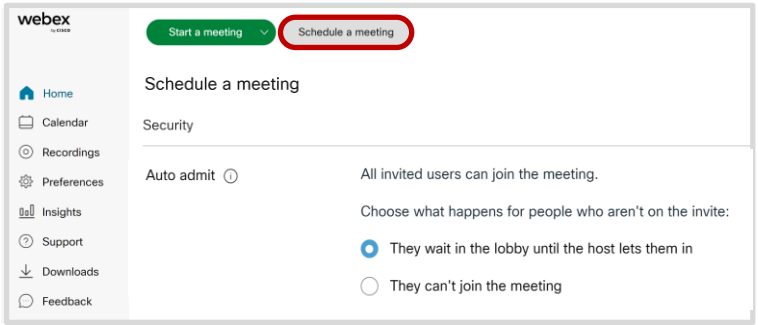
Scheduled Meetings : Auto Admit feature

Authenticated, invited users & rooms listed on the meeting owner's calendar invite can join or start the meeting with or without host

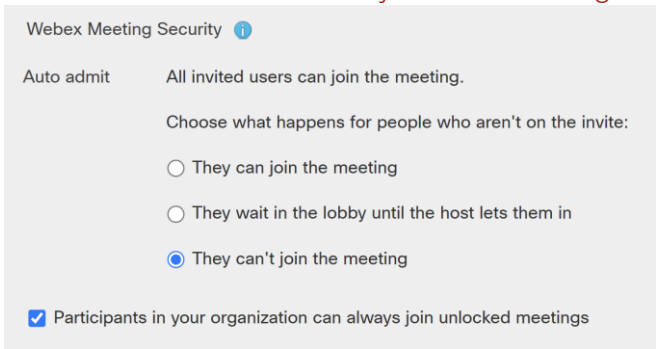
Site Admin – Uninvited Users : Wait in the Lobby until the host admits them



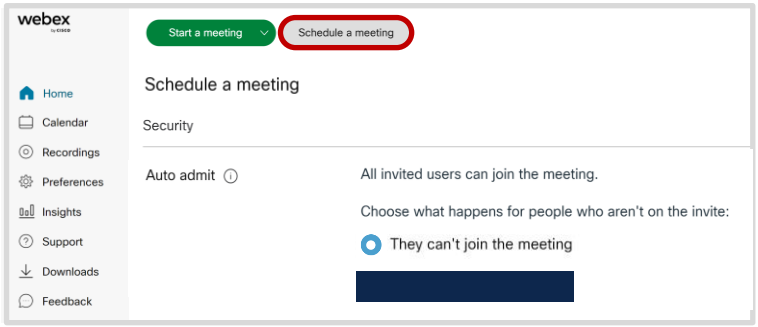
User Page : Scheduled Meeting : Auto Admit



Uninvited Users : Cannot join the meeting

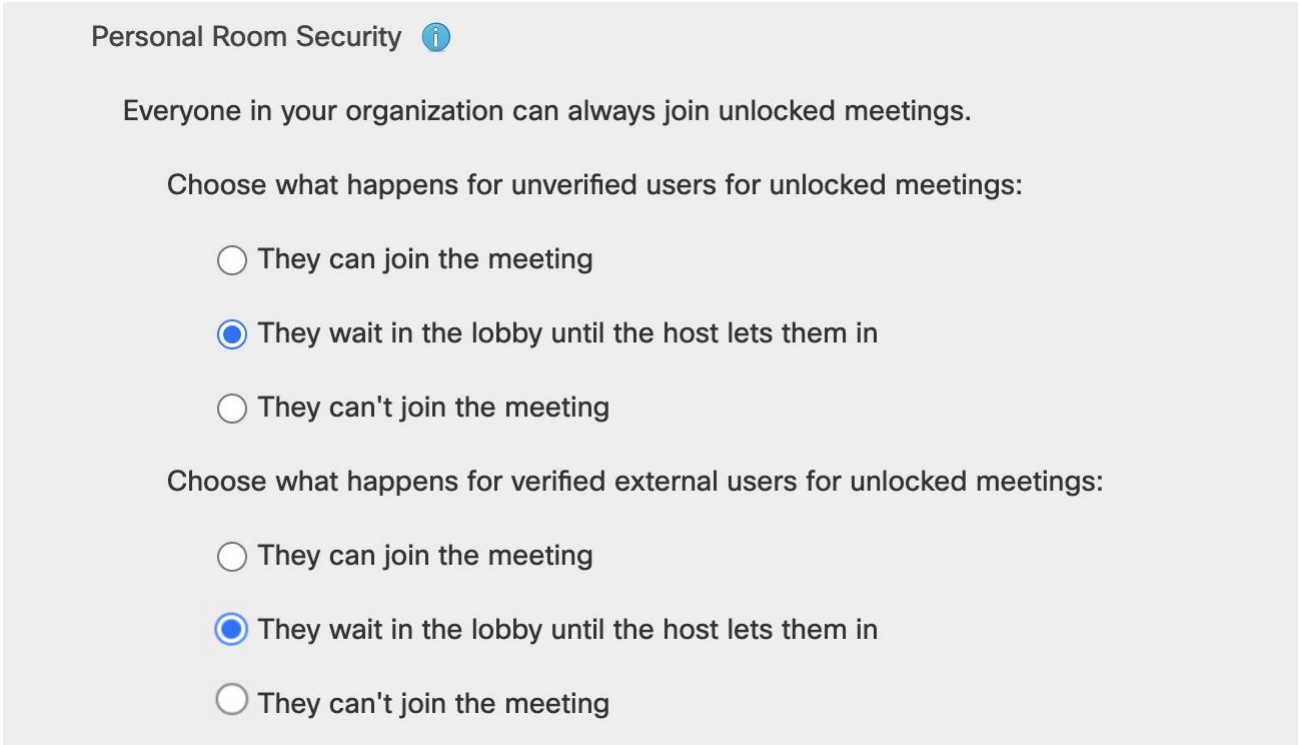


User Page : Scheduled Meeting : Auto Admit



Personal Room Meeting Lobby Controls

New : Personal Room Lobby settings



Today :
Guests = Unverified Users and verified (authenticated) External Users.

This can lead to lobby bloat in large meetings and a tendency for hosts to “admit all” rather than vet individual users

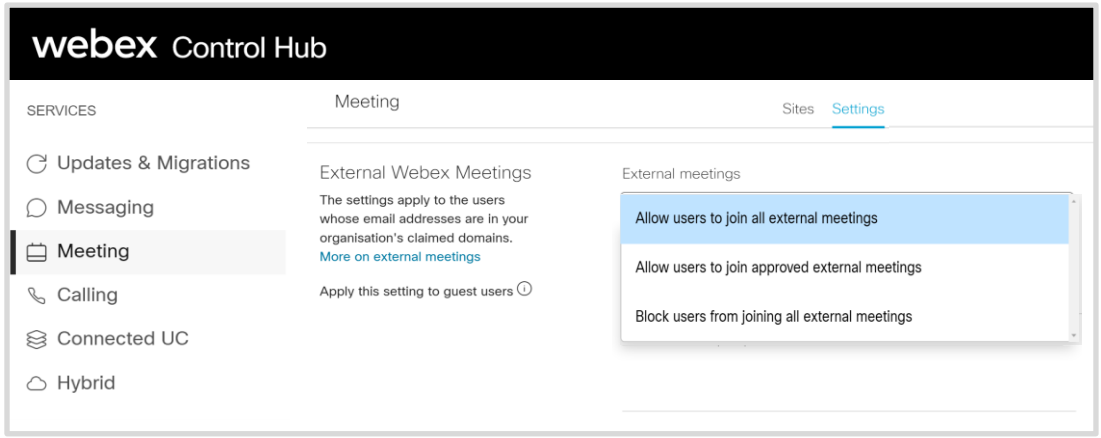
New settings :
Separate lobby controls unverified users and verified external users.

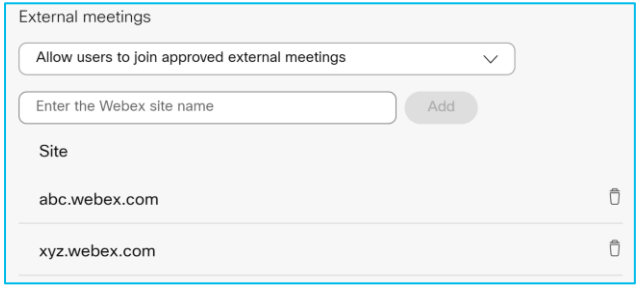
Allows administrators to apply different sets of controls for these groups of users, to reduce lobby bloat and meeting fraud

New Webex Meetings Security features

- Scheduled Meetings : Auto Admit feature
- Personal Meeting Rooms : New Lobby Controls
- Organization/ User Group/ User :
  - External Meeting Access Controls
  - Internal Meeting Access Controls
  - External Meeting Feature Controls
  - Internal Meeting Feature Controls
- Meeting Lobby/Roster/Video : Identity Labels
- Vetting Users in the Lobby – Move to breakout room

Control Hub Organization wide/User Group/User : Access Controls – External Webex Meetings





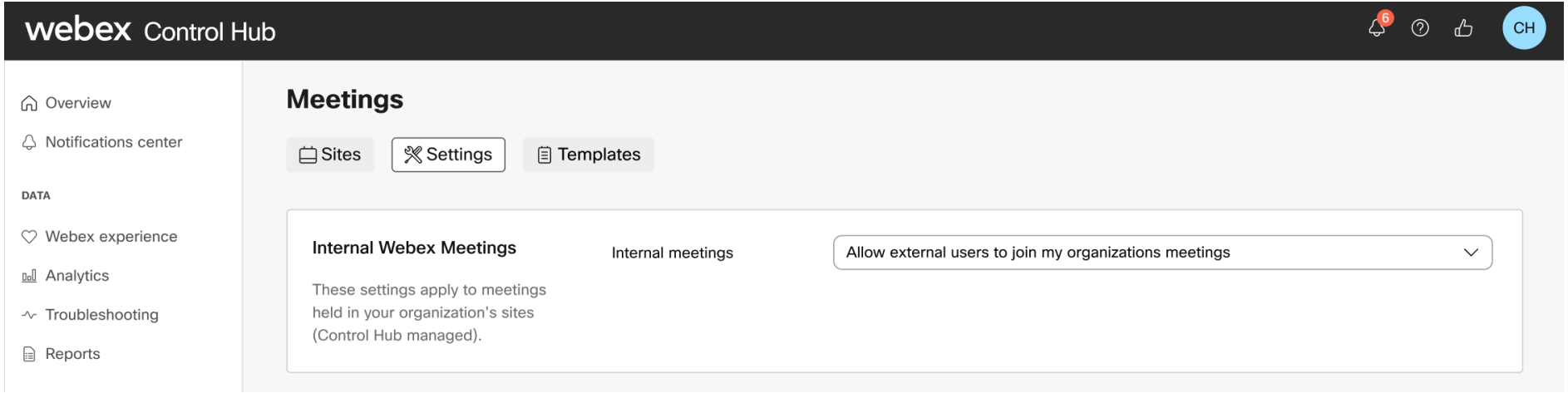
All meetings (Default setting) : Allow users to join all external meetings
Approved external sites only : All users in the org can join meetings hosted on approved external sites
Internal meetings only : Block users from joining all external meetings

These controls can be applied to :

- All users in the organization
- Groups of users – using Templates applied to user groups
- Individual users – user profile

Control Hub Organization wide/User Group/User : Internal Webex Meeting Access Controls (1)

Any external user can join Scheduled and Personal Room meetings (Default Setting)



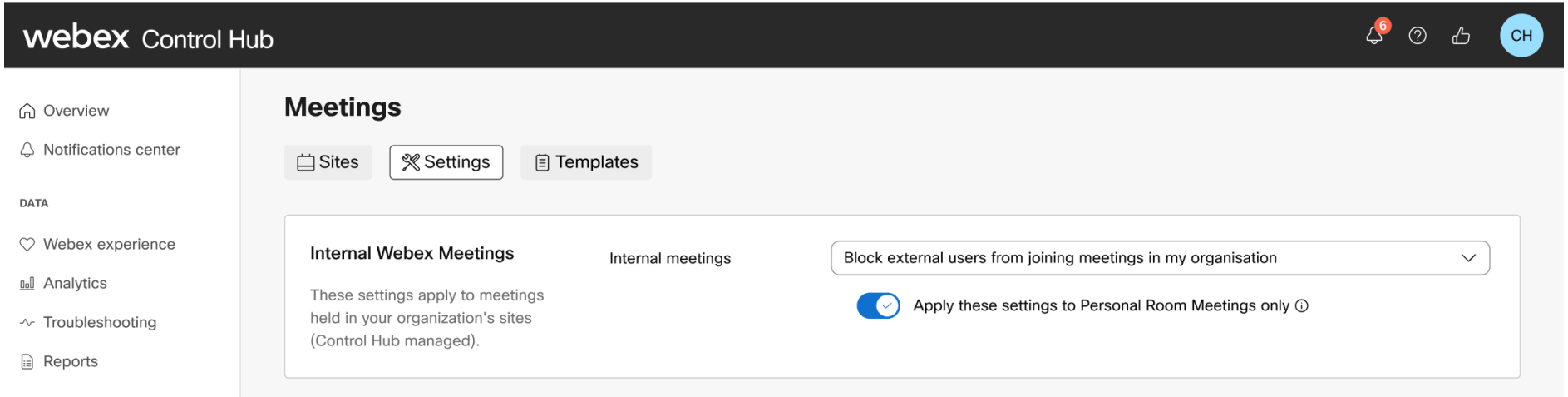
These controls can be applied to :

- All users in the organization
- Groups of users – using Templates applied to user groups
- Individual users – user profile

Control Hub Organization wide/User Group/User : Internal Webex Meeting Access Controls (2)

Option 1 : No external users can join Personal Room meetings and Scheduled meetings (default)

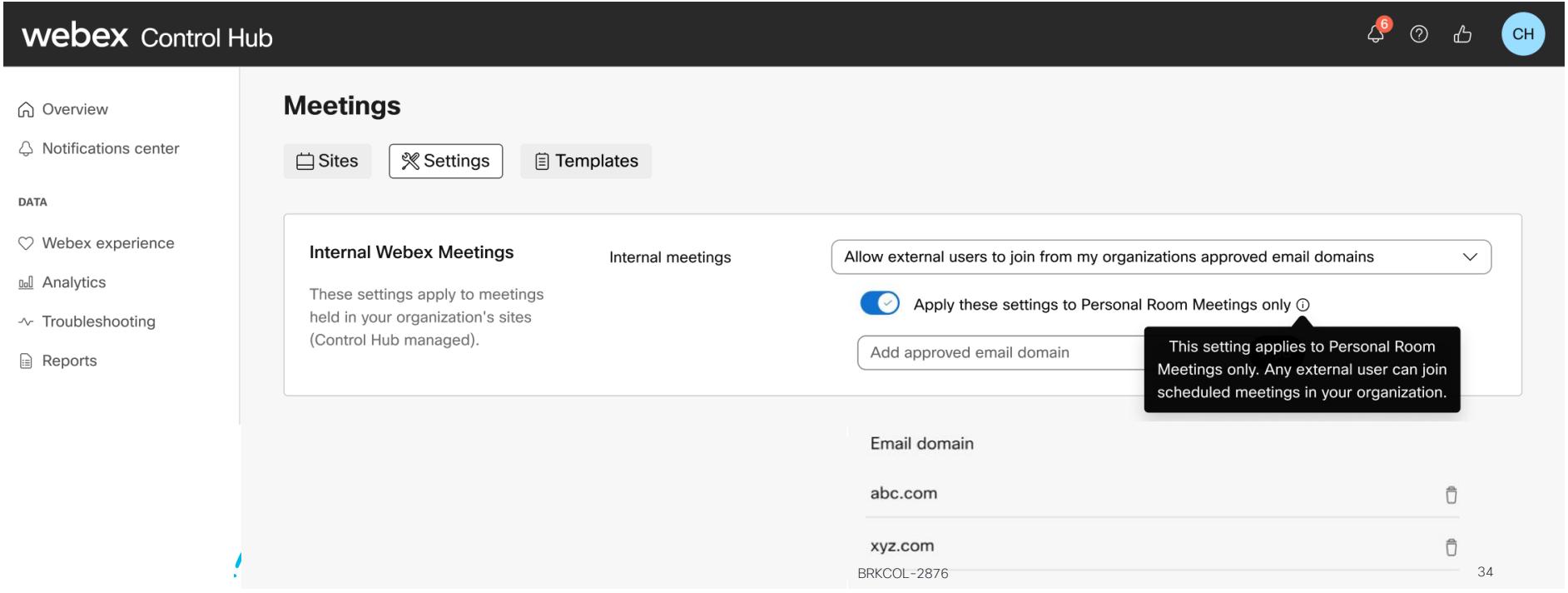
Option 2 : No external users can join Personal Room meetings Any user can join scheduled meetings



Control Hub Organization wide/User Group/User : Internal Webex Meeting Access Controls (3)

Option 1 : Only users in approved external domains can join Personal Room meetings and Scheduled meetings (default)

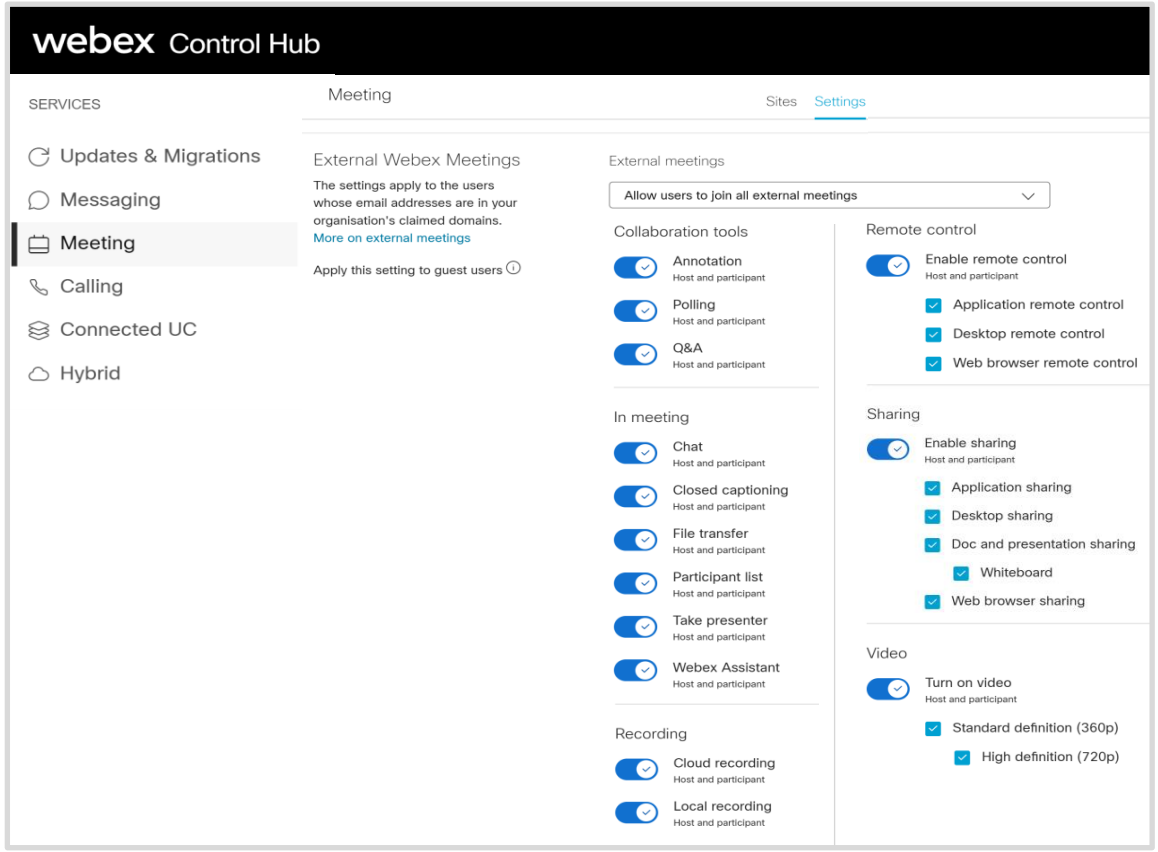
Option 2 : Only users in approved external domains can join Personal Room meetings Any user can join scheduled meetings



New Webex Meetings Security features

- Scheduled Meetings : Auto Admit feature
- Personal Meeting Rooms : New Lobby Controls
- Organization/ User Group/ User :
  - External Meeting Access Controls
  - Internal Meeting Access Controls
  - External Meeting Feature Controls
  - Internal Meeting Feature Controls
- Meeting Lobby/Roster/Video : Identity Labels
- Vetting Users in the Lobby – Move to breakout room

Feature Controls for External Webex Meetings



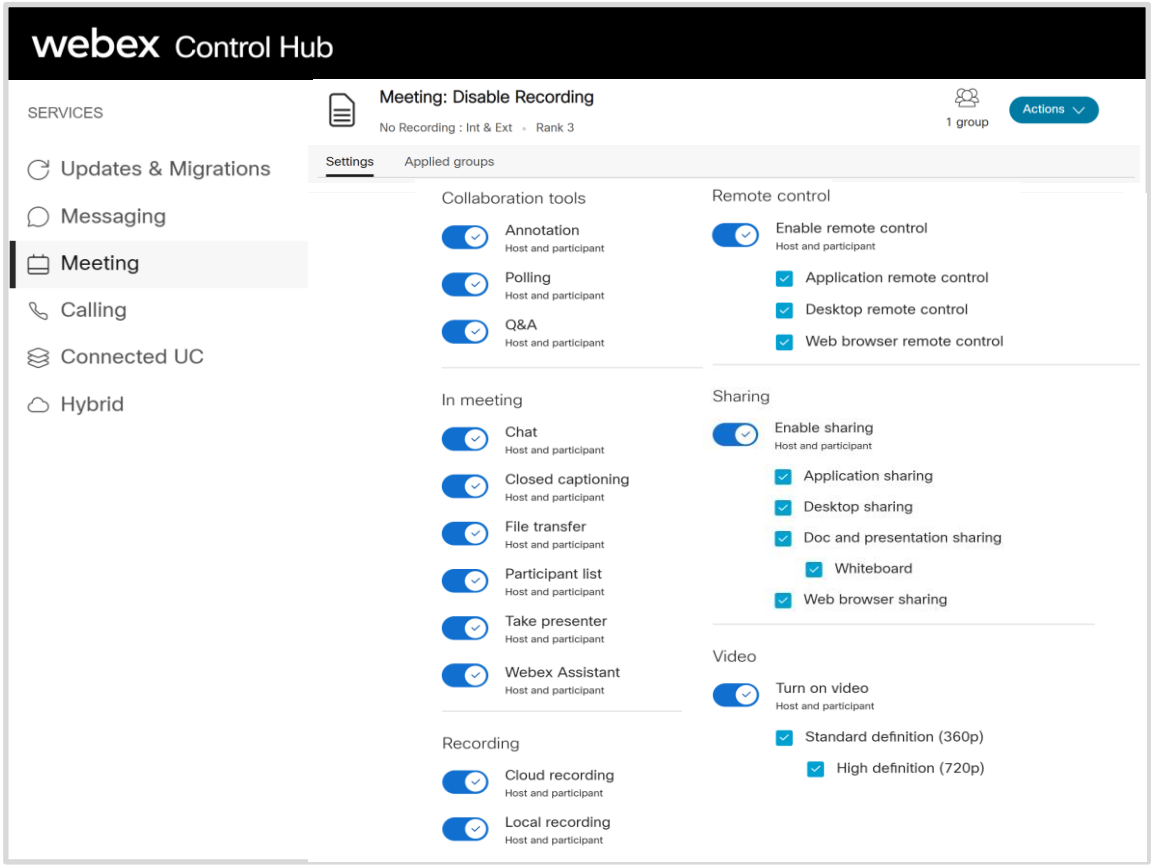
These meeting feature controls apply when users in your organization join any external Webex meeting

These controls do not apply to users joining internal meetings

These controls can be applied to :

- All users in the organization
- Groups of users – using Templates
- Individual users – user profiles

Feature Controls for Internal Webex Meetings



These meeting feature controls apply when users in your organization join any internal Webex meeting

Telephony controls (not shown)
- Call In
- Call Back
- VoIP

These controls do not apply to users joining external meetings

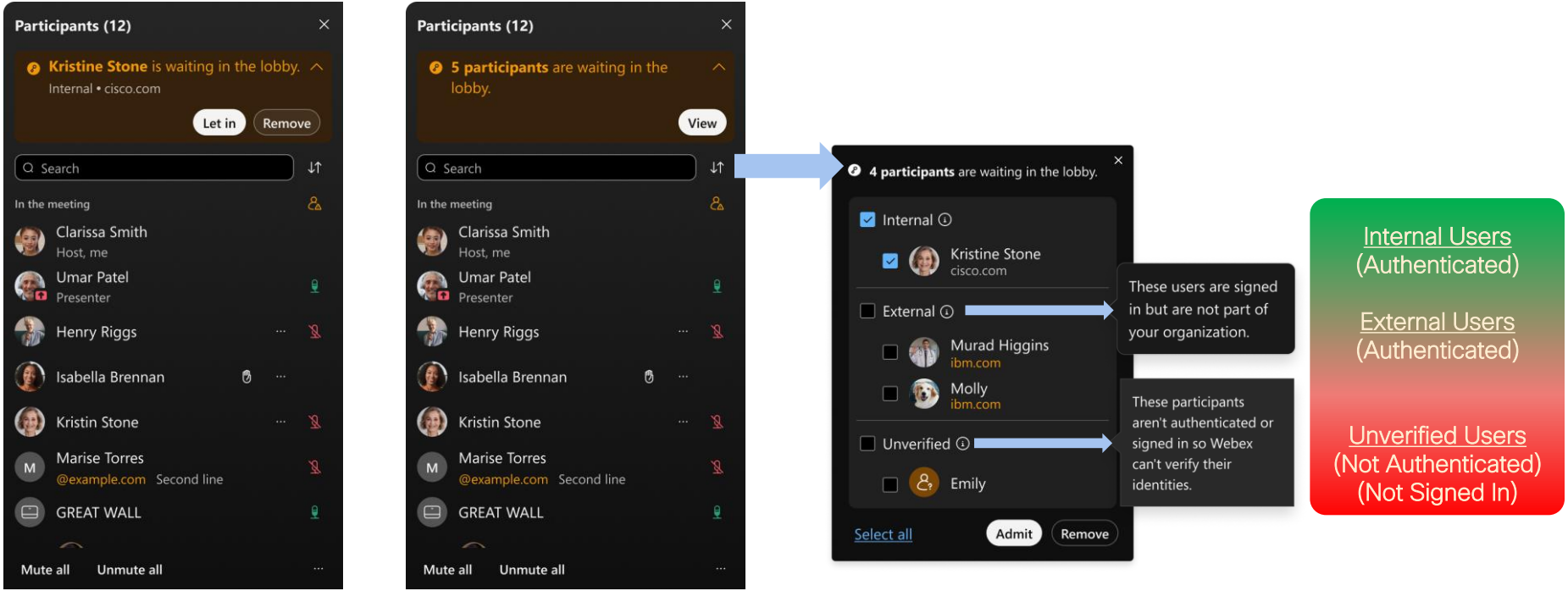
These controls can be applied to :
- All users in the organization
- Groups of users – using Templates
- Individual users – user profile

New Webex Meetings Security features

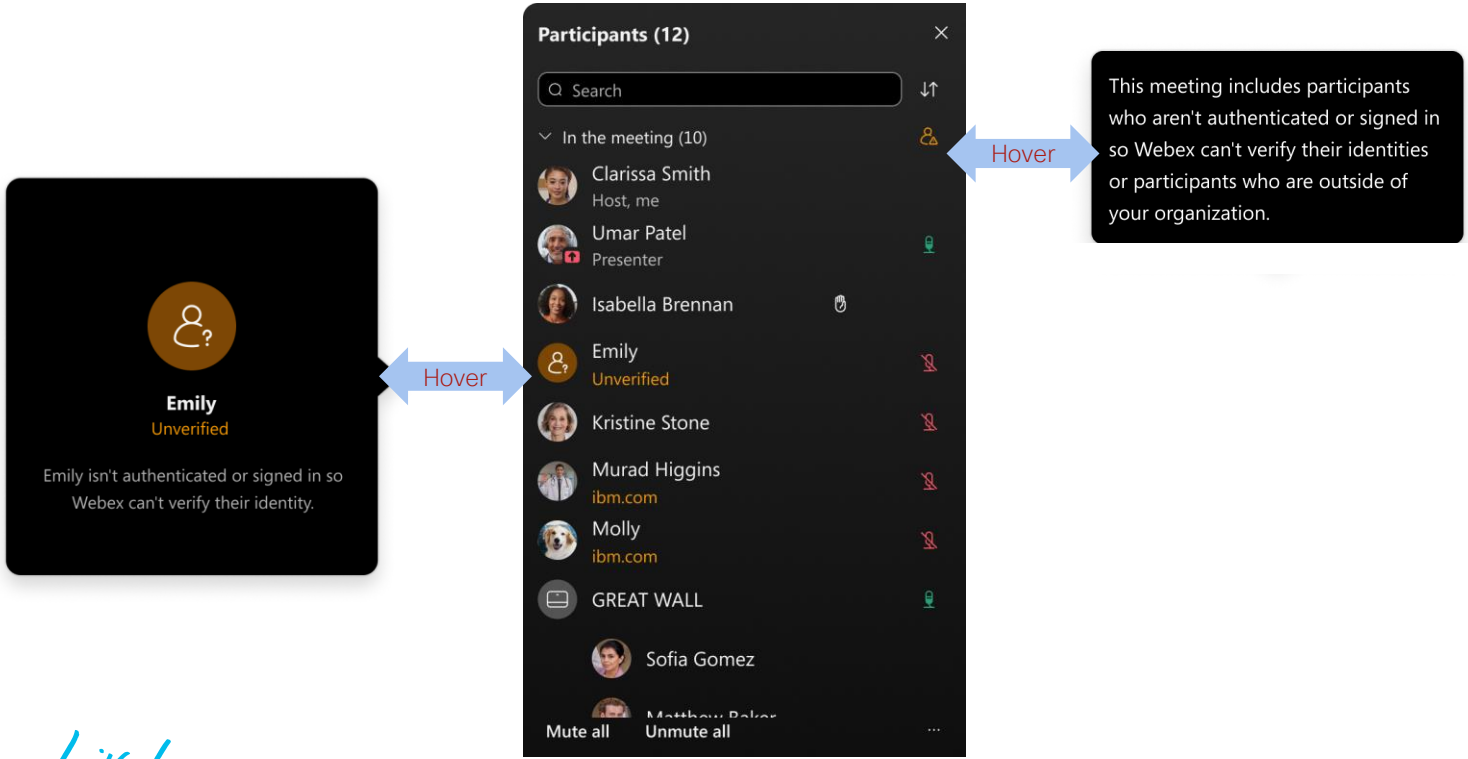
- Scheduled Meetings : Auto Admit feature
- Personal Meeting Rooms : New Lobby Controls
- Organization/ User Group/ User :
  - External Meeting Access Controls
  - Internal Meeting Access Controls
  - External Meeting Feature Controls
  - Internal Meeting Feature Controls
- Meeting Lobby/Roster/Video : Identity Labels
- Vetting Users in the Lobby – Move to breakout room

Webex Meetings : Host Controls

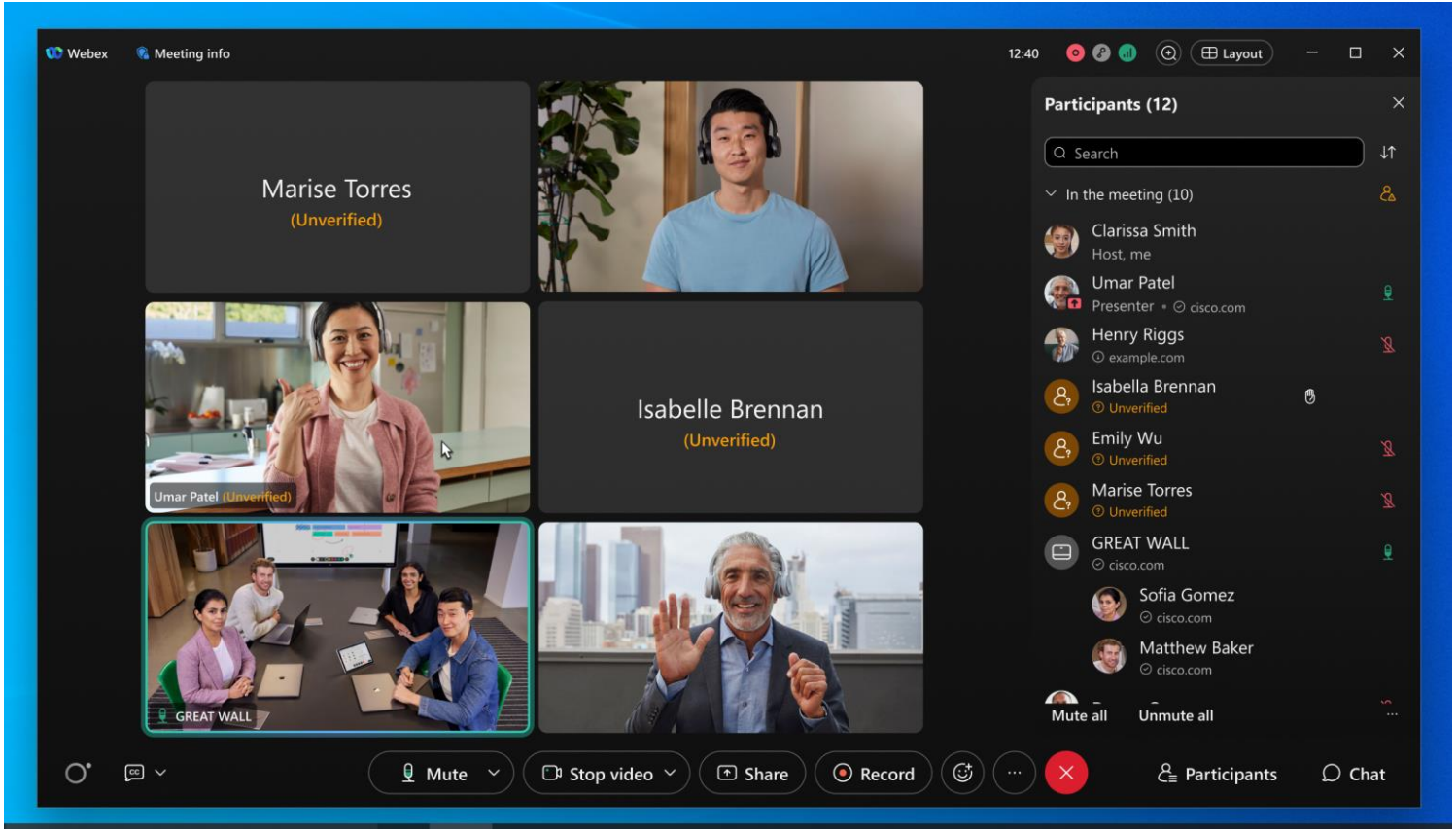
Admitting Users from the Lobby
Lobby : User Categories and User Identity information



Webex Meetings : In Meeting Participant Roster Participant Identity Information

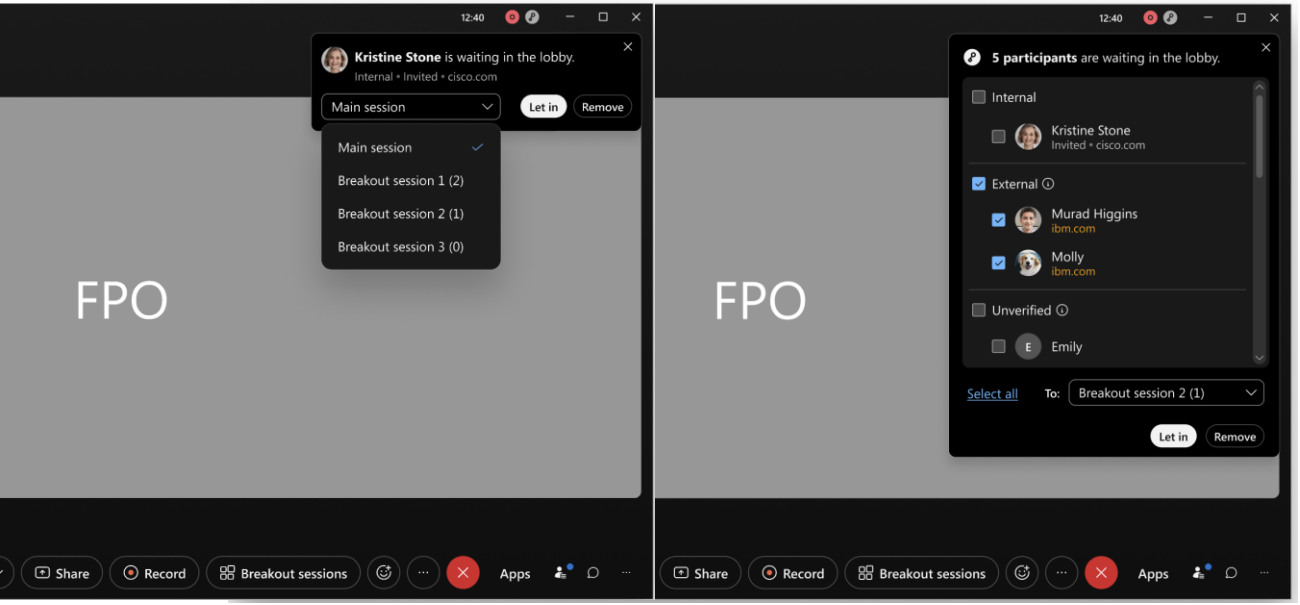


Video Display : User Identity information

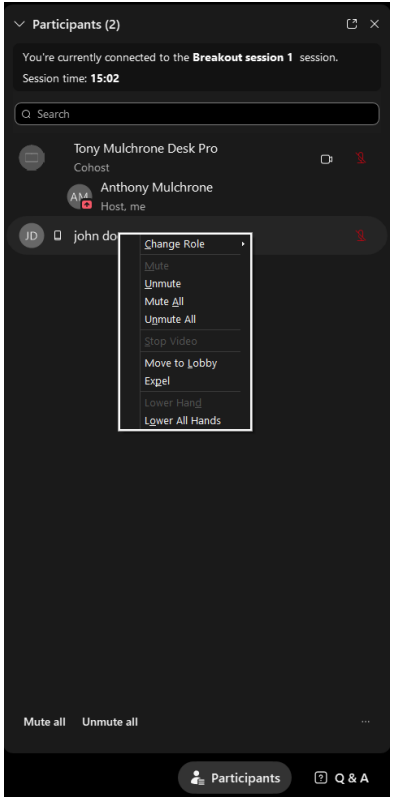


Using a breakout room to vet users in the Lobby

Move users from Lobby to Breakout room



Move or Expel users



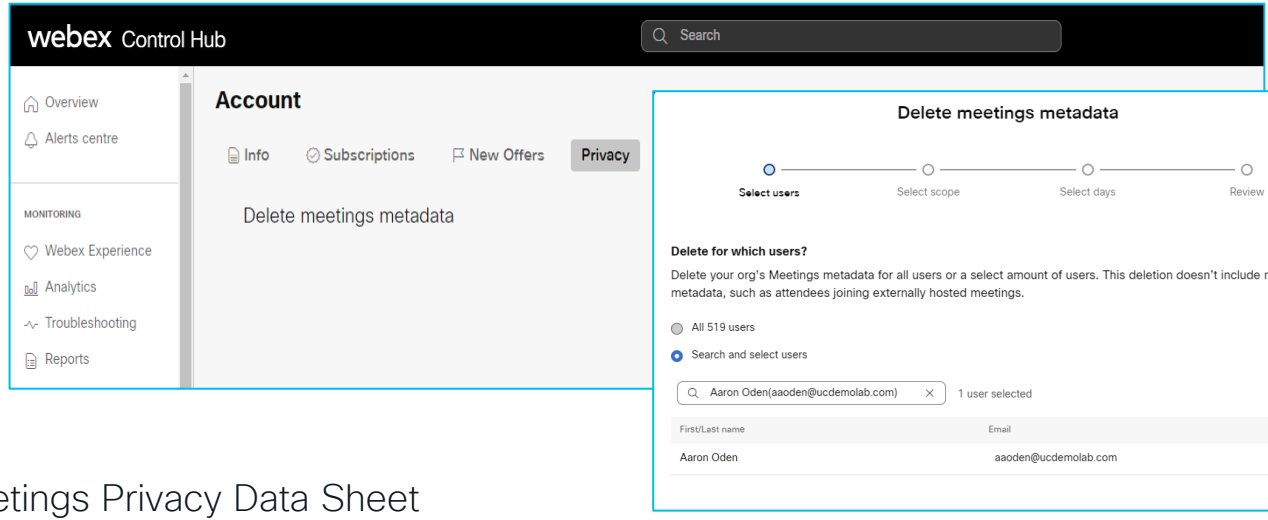
New Webex Meetings features : Privacy

Delete Meeting Host and Usage information

Webex Meetings – Delete Meeting Host and Usage data

Webex Meetings : Host and Usage data examples

IP Address
User Agent Identifier
Hardware Type
Operating System Type & Version
Client Version…..
Host Name and email address
Meeting Site URL
Meeting Start/End Time
Meeting Title
Call attendee information



For full details see the Webex Meetings Privacy Data Sheet
https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf

Control Hub -> Account -> Privacy

Allows and administrator to delete Meeting Host and Usage Information based on Meeting Host name
Deleted data cannot be retrieved
https://help.webex.com/en-us/article/l4pqoi/Delete-Webex-Meetings-host-and-usage-information-of-users-in-Control-Hub

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Complete your Session Survey

- 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 (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN