



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 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

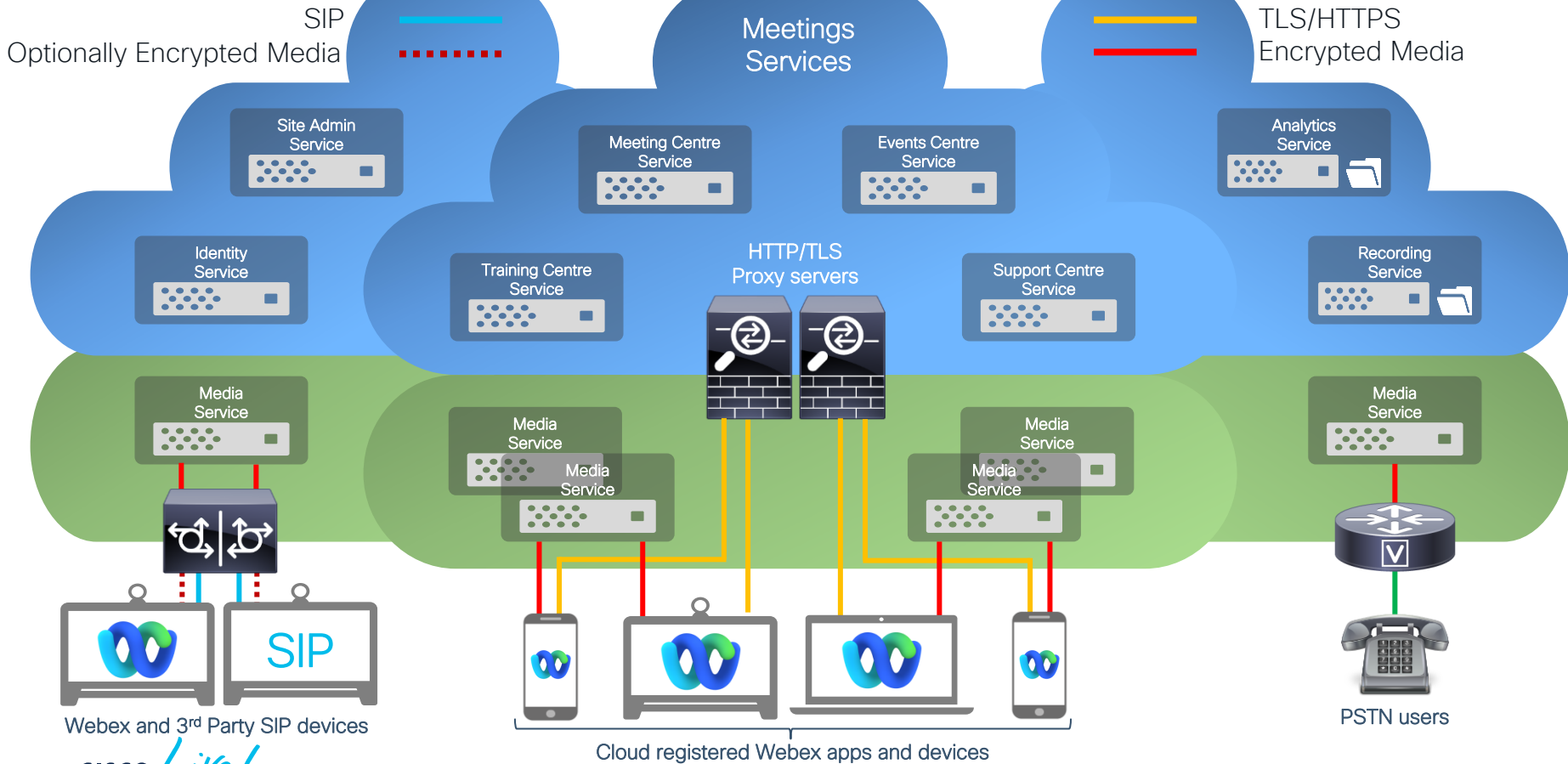
Webex spaces will be moderated until February 24, 2023.



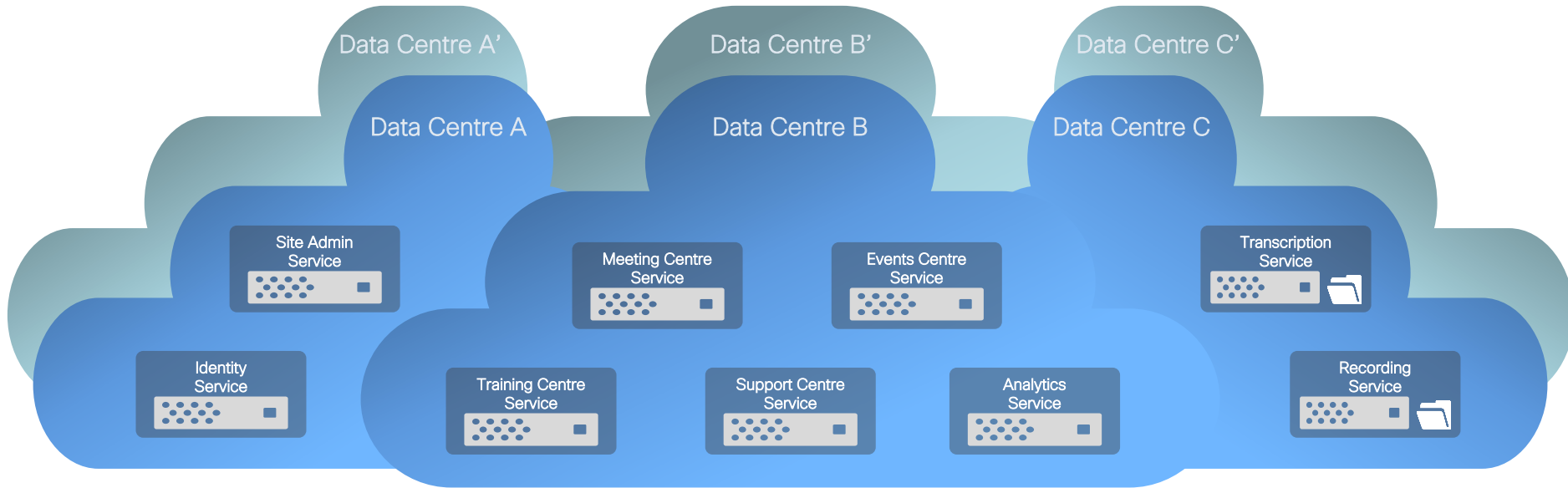
Agenda

- 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

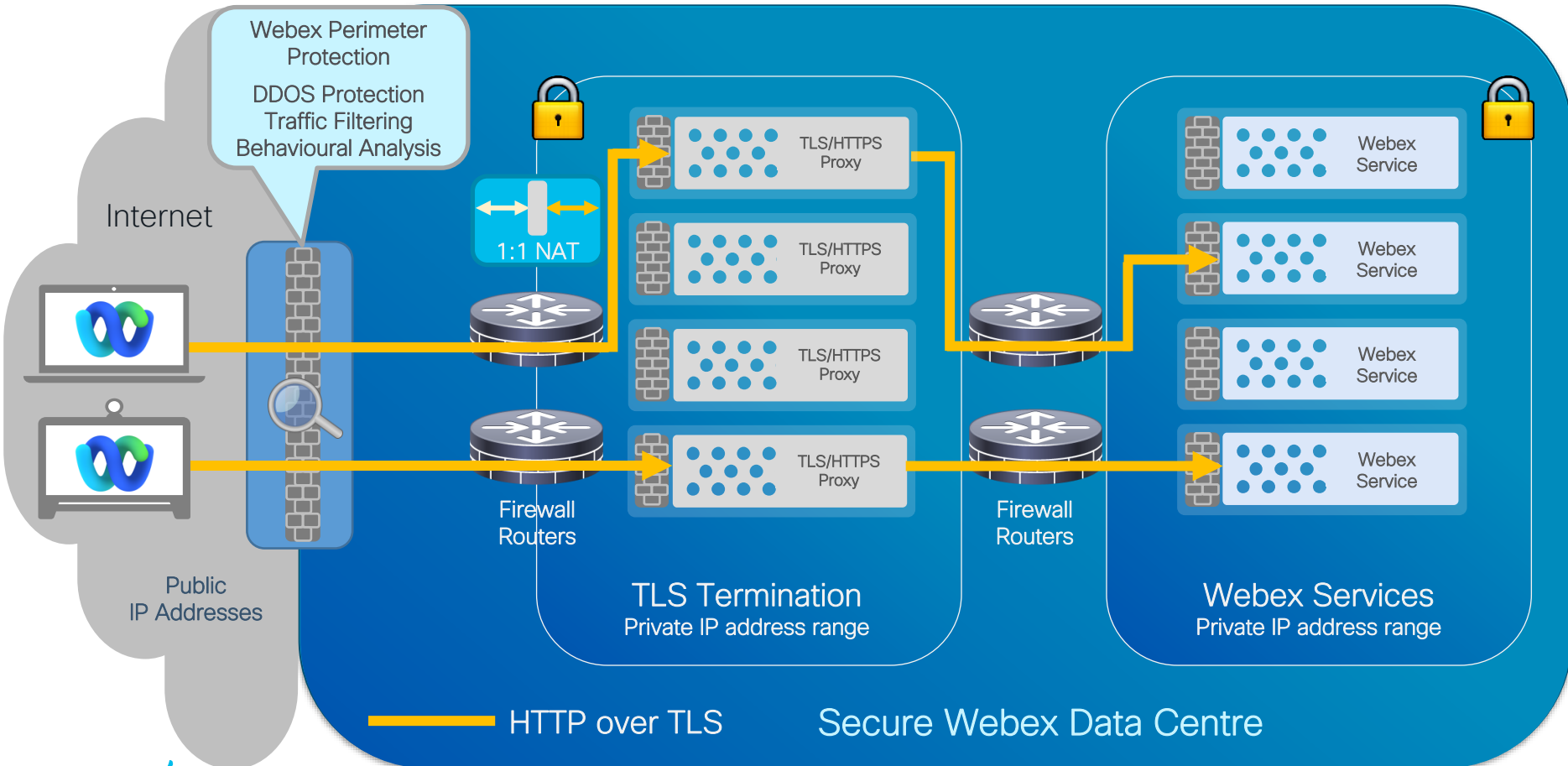
Webex Meetings : Secure Platform

- TLS signalling
- Encrypted Media

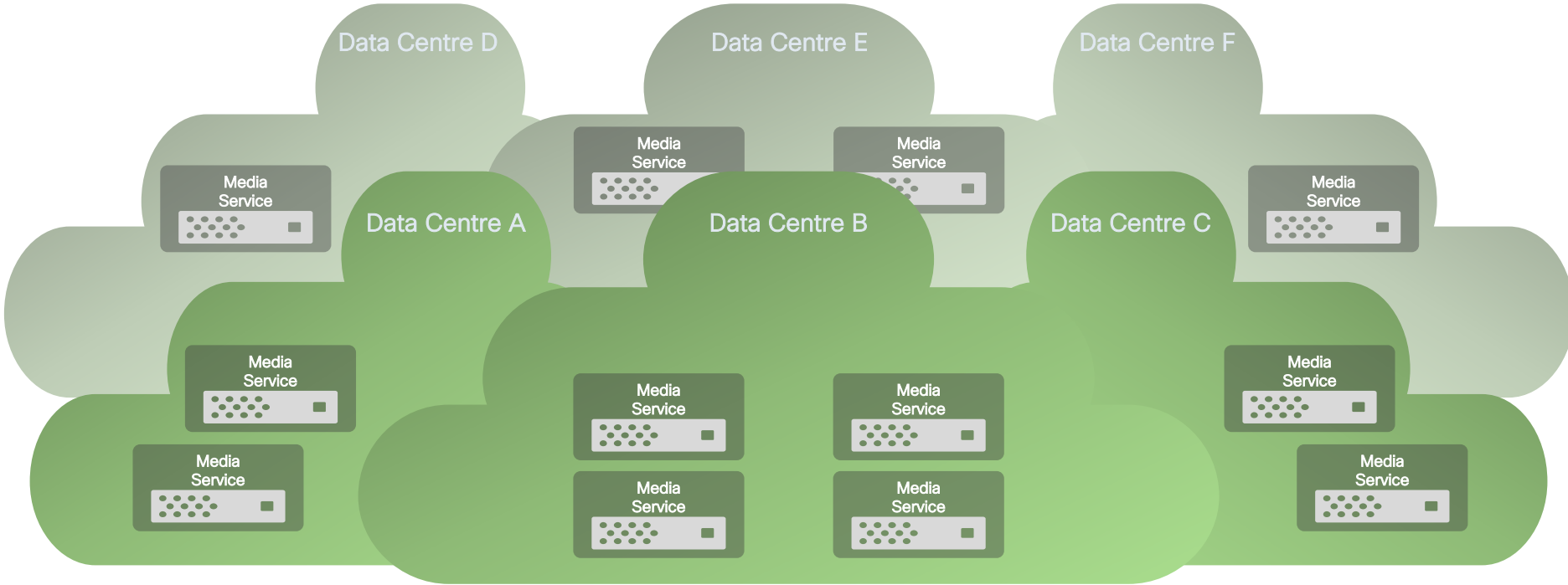
Network Requirements for Webex Meetings and Messaging services
<https://help.webex.com/en-us/WBX000028782>



Webex encrypted HTTP signaling – TLS/HTTPS traffic

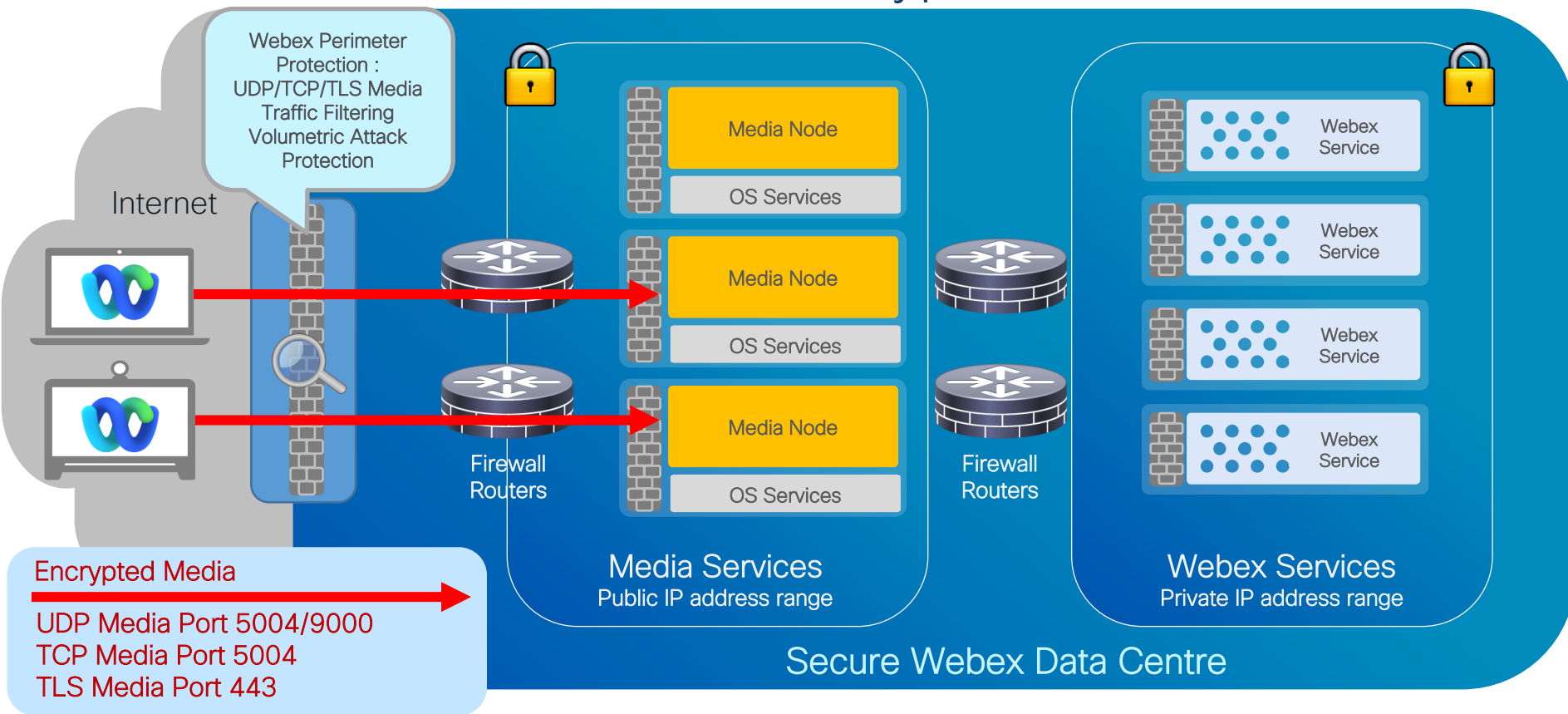


Webex Media Services

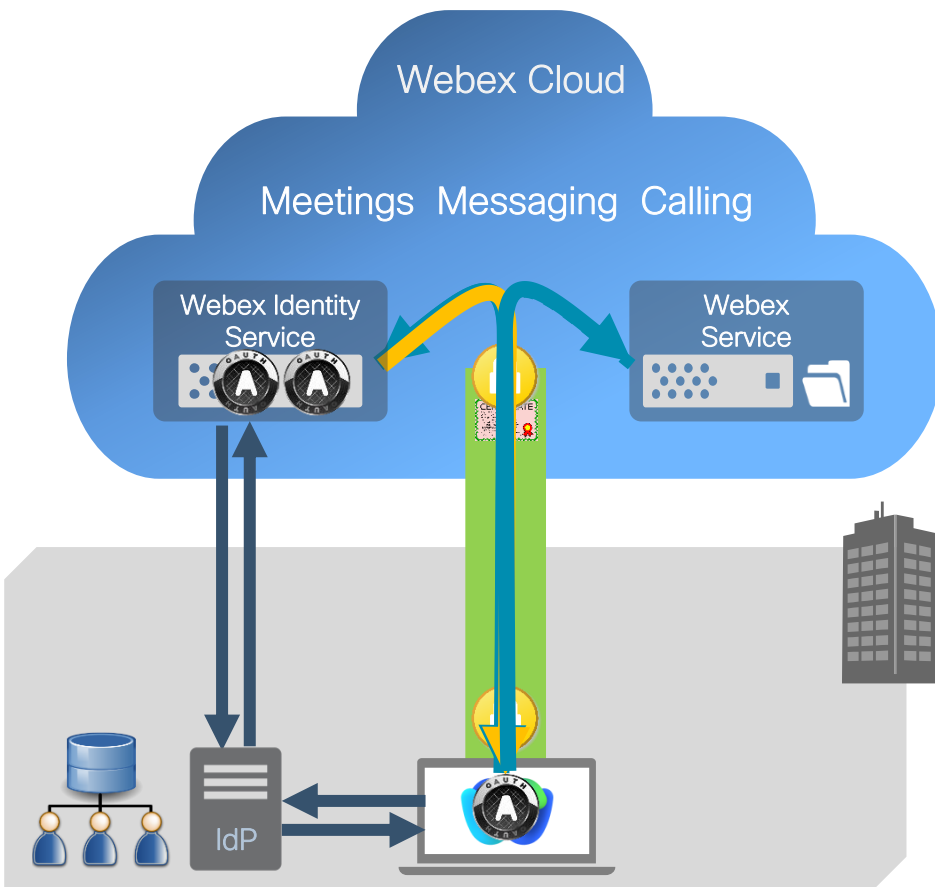


Webex Media services are globally distributed across multiple data centres
Media Server clusters in each data centre provide local and geographic redundancy
Media servers support voice, video and content sharing
All media is encrypted

Webex Media Services : Encrypted Media



Webex 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

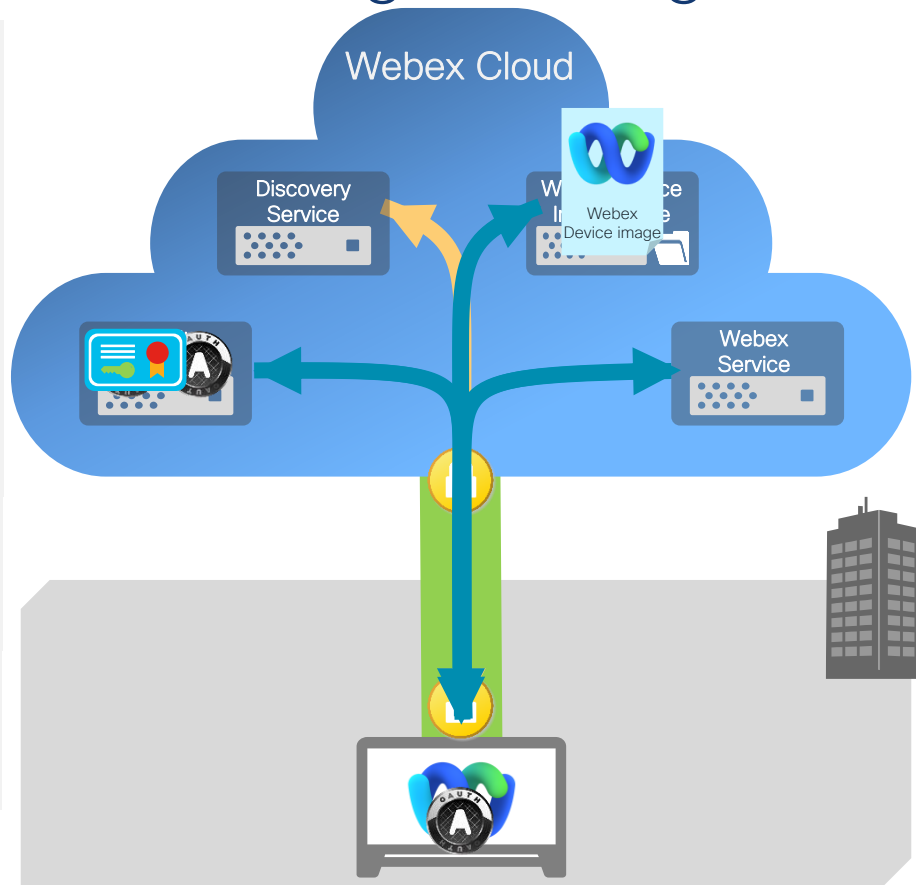
Webex Control Hub administrator generates device activation code for the device

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



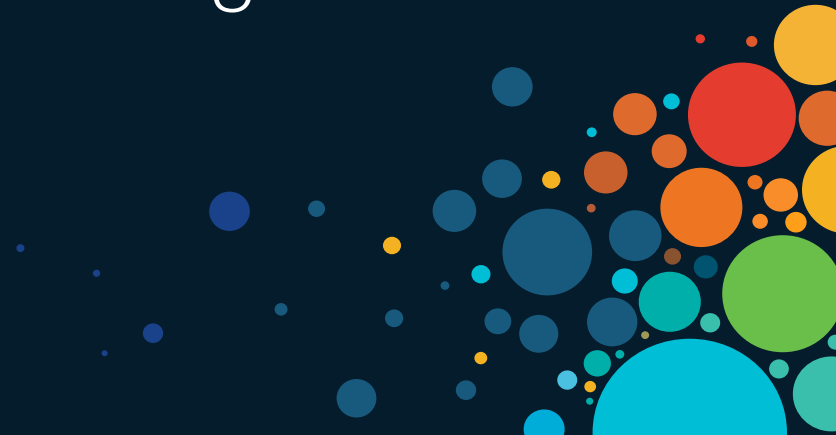
1234567890123456

* Can include Enterprise CA Certs for TLS Proxy inspection

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

The screenshot shows the Webex Control Hub interface for 'Test User 1'. The 'Meetings' tab is selected, showing the 'Session types' section. The 'Webex Meetings' limit is set to 1000. Three session types are listed, all with enabled toggle switches:

Session types	Webex Meetings Limit: 1000	Toggle	Session Type
		On	STD Standard Meeting
		On	PRO Private Meeting (Video Mesh only)
		On	PRO Pro End to End Encrypted (VOIP only)

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

Schedule a meeting

Meeting type ⓘ

Webex Meetings Standard meeting

* Meeting topic

Webex Meetings Private Meeting (Video Mesh only)

Webex Meetings Pro-End to End Encryption_VOIPonly

Date and time

Webex Meetings Standard meeting

Encryption for standard Webex Meetings

With standard Webex Meetings, all signalling and media in the Webex cloud is encrypted

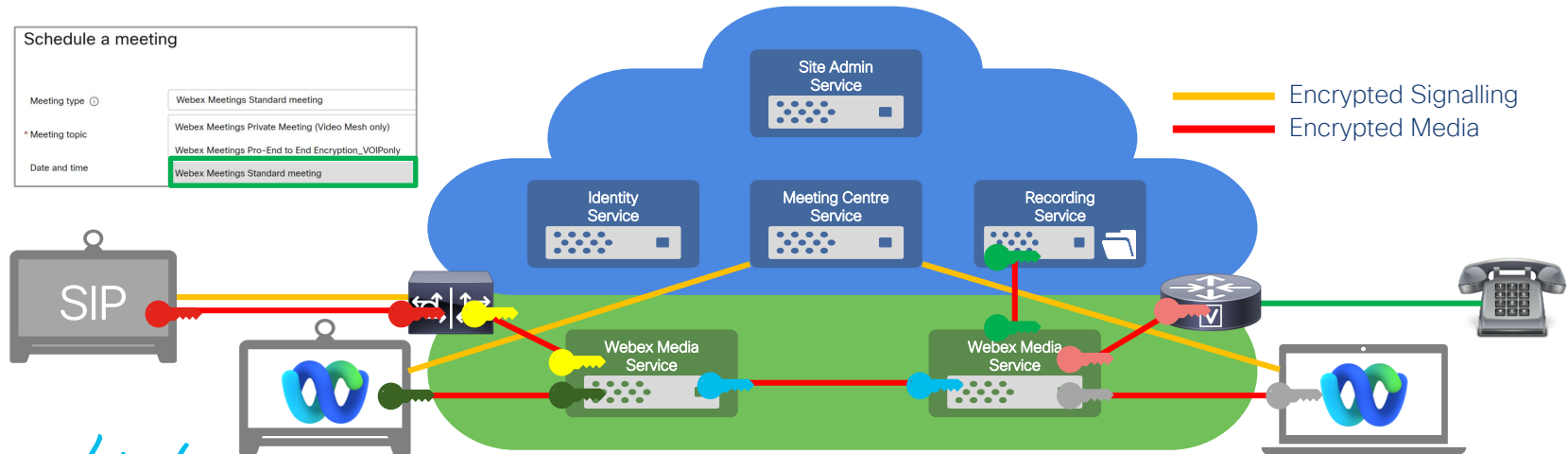
Webex apps and devices use encrypted signalling and encrypted media

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)



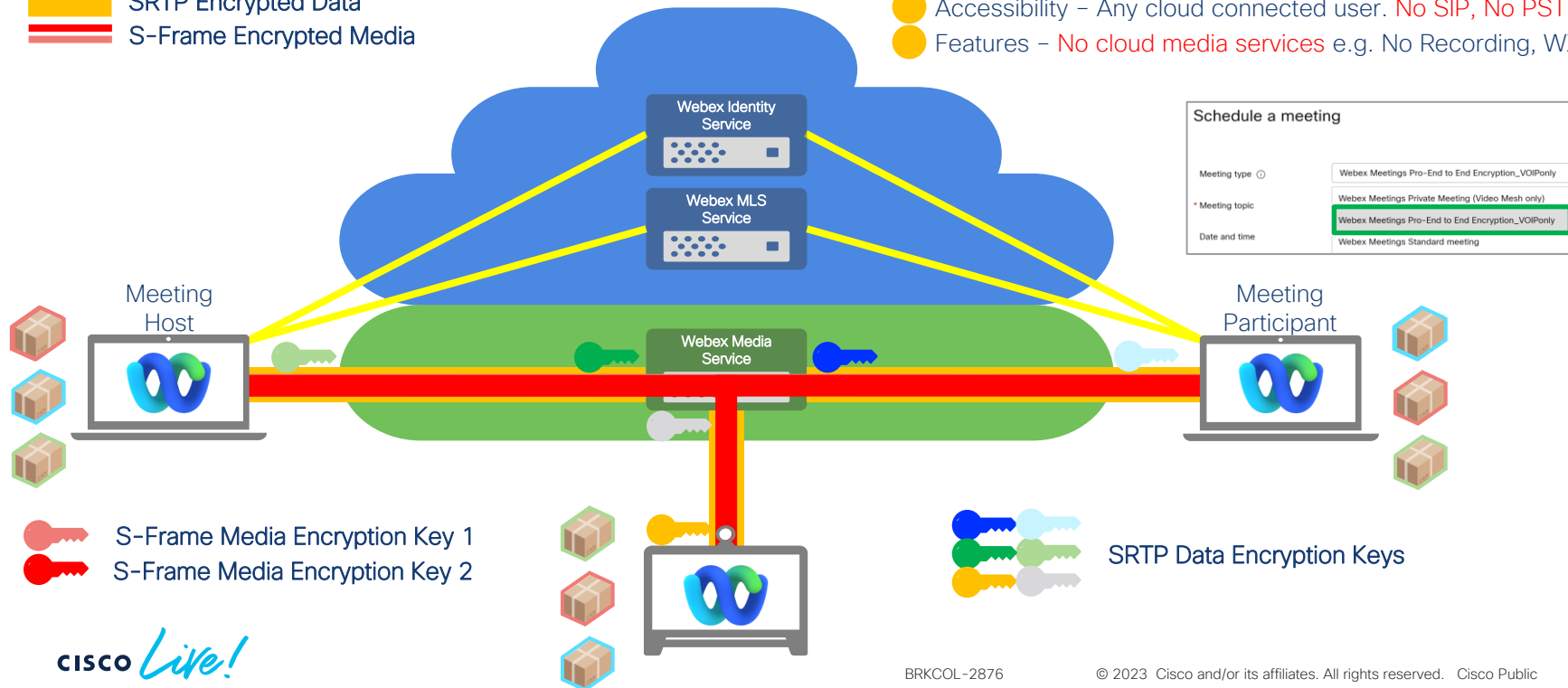
Webex Zero Trust End to End Encrypted Meetings

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
- S RTP 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

Schedule a meeting

Meeting type ⓘ

- Webex Meetings Private Meeting (Video Mesh only)
- Webex Meetings Private Meeting (Video Mesh only)**
- Webex Meetings Pro-End to End Encryption_VOIPOnly
- Webex Meetings Standard meeting

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

Meeting type ⓘ

Webex Meetings Private Meeting (Video Mesh only) ▼

This is a private meeting. All attendees must be members of the host organization and must be connected to its corporate network. They can only join the meeting from the Webex app or from an authenticated video system in the host organization.

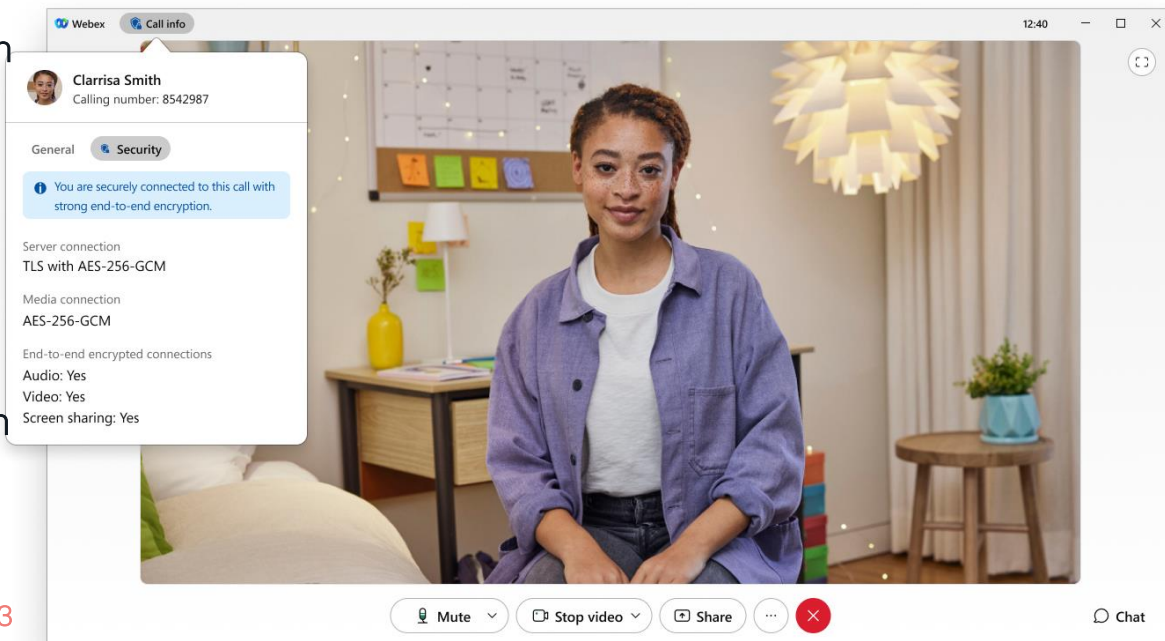


Zero Trust Security for one-to-one calls

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

The screenshot shows the 'Security' settings for a Webex meeting. The 'Meeting password' field contains 'sPmjBmc*839'. Under 'Exclude password', the option 'Exclude password from email invitation' is unchecked. The 'Automatic lock' section shows 'Automatically lock my meeting' set to 15 minutes after the meeting starts. The 'Unlocked meetings' section indicates that everyone in the organization can join unlocked meetings, and when the meeting is unlocked, 'Guests wait in the lobby until the host admits them' is selected. The 'Join before host' section shows 'Attendees can join the meeting' set to 5 minutes before start time, and 'Attendees can connect to audio before start time' is unchecked. The 'Advanced options' section is expanded, showing 'view thumbnails', 'View any document', and 'View any page' all unchecked, and 'Contact operator privately' checked. Under 'Participate in private chat with', 'Host', 'Presenter', and 'Other participants' are all checked. 'Cancel' and 'OK' buttons are at the bottom right.

Security

* Meeting password: sPmjBmc*839

Exclude password: ☐ Exclude password from email invitation

Automatic lock: ☐ Automatically lock my meeting 15 minutes after the meeting starts.

Unlocked meetings: Everyone in your organization can always join unlocked meetings.
When the meeting is unlocked,
☐ Guests can join the meeting
☒ Guests wait in the lobby until the host admits them
☐ Guests can't join the meeting

Join before host: ☐ Attendees can join the meeting 5 minutes before start time
☐ Attendees can connect to audio before start time

Advanced options

☐ view thumbnails
☐ View any document
☐ View any page
☒ Contact operator privately

Participate in private chat with

☒ Host
☒ Presenter
☒ Other participants

Cancel OK

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

General

My Personal Room

Audio and Video

Scheduling

Recording

Please note that your host PIN can now be found under the **Audio and Video** section.

Personal Room name

Tony Mulchrone's Personal Room

Your Personal Room name must be between 1 and 128 characters

Personal Room link

https://.webex.com/meet/abcdefgh

Automatic lock: ⓘ

☒ Automatically lock my meeting

15

minutes after the meeting starts.

⚠ Based on your site settings, people who haven't signed in and external guests will be kept in the lobby until you admit them, whether your Personal Room is locked or unlocked.

Notification: ⓘ

☐ Notify me by email when someone enters my Personal Room lobby while I am away

Cohosts: ⓘ

☒ Allow cohosts for my Personal Room meetings

Separate email addresses with a comma or semicolon

Mute attendees ⓘ

☐ Allow the host and cohosts to unmute participants (Moderated unmute mode)

☒ Allow attendees to unmute themselves in the meeting

☐ Always mute attendees when they join the meeting

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
<u>Cloud registered Webex devices</u> <ul style="list-style-type: none">• Audio/ Video/ Desktop share• Meeting Roster, Reactions,• One Button to Push, Noise Reduction• Webex Assistant, Closed Captions• Recording etc	<u>Cloud registered Webex device security</u> Webex recognizes cloud registered devices and can apply security privileges such as Lobby bypass
<u>SIP devices</u> <ul style="list-style-type: none">• Audio/ Video/ Desktop share	<u>Security for SIP devices & Phone users</u> DTMF entered – meeting number & numeric password
<u>PSTN/ IP Phones</u> <ul style="list-style-type: none">• Audio only	<u>Video system settings :</u> Enforce numeric meeting password when joining <u>Phone settings :</u> 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>

We recommend using the following features for protection of your meetings:

Use Scheduled Meetings for comprehensive security	▼
All Meetings: Lock meetings after a default time	▼
All meetings: Use the lobby to control meeting access for guest users	▼
Scheduled meetings: Enforce meeting password when joining from phone or video conferencing systems	▼
Scheduled meetings: Don't allow attendees to join before the meeting host	▼
Personal Room meetings: Use CAPTCHA for guests joining Personal Room meetings	▼
All meetings: Disable callback to certain countries	▼
All meetings: Make all meetings unlisted	▼
All meetings: Control content sharing and file transfer	▼
All meetings: Make all meetings accessible only to users in your site, by requiring sign-in when joining a meeting, webinar, event, or training session	▼
All meetings: Hide meeting link from attendees within meetings	▼
All meetings: Disable virtual cameras	▼
Account management	▼

Webex best practices for secure meetings: hosts

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

Best practices for hosts

As a host, you're the final decision maker concerning the security settings of your meetings, events, webinars, and training sessions. You control nearly every aspect of the meeting, event, webinar, or training session, including when it begins and ends.

Keep your meetings and information secure. Know and follow the security policies for your organization. Follow security best practices when you schedule a meeting, during a meeting, and after a meeting.

 Use Meeting Lobby and Auto Lock controls when available.

Don't publish passwords to publicly accessible websites.

Don't share your Audio PIN with anyone.

Provide meeting passwords only to users who need them.

Never share sensitive information in your meeting until you're certain who is in attendance.

Securing your Personal Room	▼
Securing Scheduled Meetings	▼
Security during the meeting	▼
Security after the meeting	▼

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.....



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

Webex Meeting Security ⓘ

Auto admit All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☐ They can join the meeting

☒ They wait in the lobby until the host lets them in

☐ They can't join the meeting

☒ Participants in your organization can always join unlocked meetings



User Page : Scheduled Meeting : Auto Admit

webex

Start a meeting Schedule a meeting

Schedule a meeting

Security

Auto admit ⓘ All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☒ They wait in the lobby until the host lets them in

☐ They can't join the meeting

Uninvited Users : Cannot join the meeting

Webex Meeting Security ⓘ

Auto admit All invited users can join the meeting.

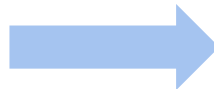
Choose what happens for people who aren't on the invite:

☐ They can join the meeting

☐ They wait in the lobby until the host lets them in

☒ They can't join the meeting

☒ Participants in your organization can always join unlocked meetings



User Page : Scheduled Meeting : Auto Admit

webex

Start a meeting Schedule a meeting

Schedule a meeting

Security

Auto admit ⓘ All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☒ They can't join the meeting

Personal Room Meeting Lobby Controls

New : Personal Room Lobby settings

Personal Room Security ⓘ

Everyone in your organization can always join unlocked meetings.

Choose what happens for unverified users for unlocked meetings:

- ☐ They can join the meeting
- ☒ They wait in the lobby until the host lets them in
- ☐ They can't join the meeting

Choose what happens for verified external users for unlocked meetings:

- ☐ They can join the meeting
- ☒ They wait in the lobby until the host lets them in
- ☐ They can't join the meeting

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.

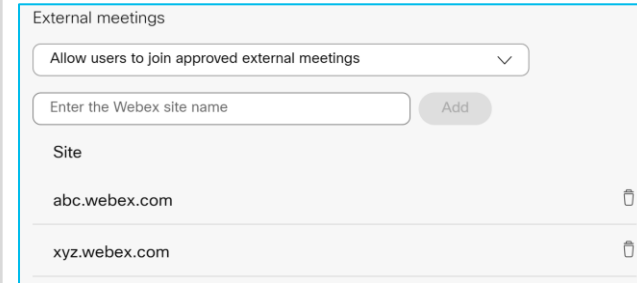
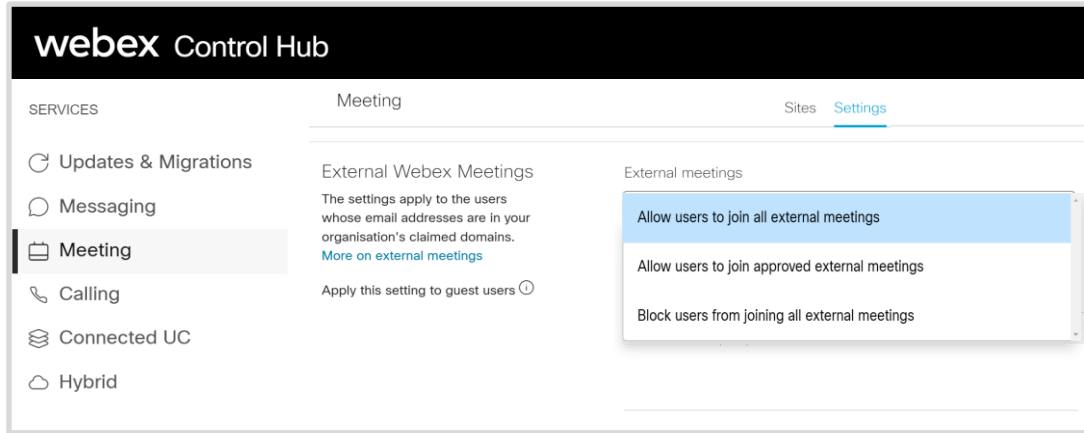
Allows administrators to apply different sets of controls for these groups of users, to reduce lobby bloat and meeting fraud

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)

The screenshot displays the Webex Control Hub interface. The top navigation bar includes the 'webex Control Hub' logo, a notification bell with a red '6' badge, a help icon, a thumbs-up icon, and a 'CH' profile button. The left sidebar contains navigation links: Overview, Notifications center, DATA, Webex experience, Analytics, Troubleshooting, and Reports. The main content area is titled 'Meetings' and features three tabs: Sites, Settings (which is active), and Templates. Under the 'Settings' tab, there is a section for 'Internal Webex Meetings' with the subtitle 'Internal meetings'. A dropdown menu is set to 'Allow external users to join my organizations meetings'. Below this, a note states: 'These settings apply to meetings held in your organization's sites (Control Hub managed)'.

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

The screenshot displays the Webex Control Hub interface. At the top, the 'webex Control Hub' header is visible on the left, and on the right, there are icons for notifications (with a red '5' badge), help, feedback, and a user profile icon labeled 'CH'. A left-hand navigation menu includes 'Overview', 'Notifications center', 'DATA', 'Webex experience', 'Analytics', 'Troubleshooting', and 'Reports'. The main content area is titled 'Meetings' and contains three tabs: 'Sites', 'Settings' (which is active), and 'Templates'. Under the 'Settings' tab, there is a section for 'Internal Webex Meetings' with the subtitle 'Internal meetings'. A dropdown menu is open, showing the option 'Block external users from joining meetings in my organisation'. Below this, a toggle switch is turned on, with the text 'Apply these settings to Personal Room Meetings only' and a help icon.

webex Control Hub

Meetings

Internal Webex Meetings Internal meetings

Block external users from joining meetings in my organisation

These settings apply to meetings held in your organization's sites (Control Hub managed).

Apply these settings to Personal Room Meetings only

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

The screenshot displays the Webex Control Hub interface. The top navigation bar includes the 'webex Control Hub' logo and icons for notifications (6), help, feedback, and a user profile (CH). The left sidebar contains navigation links: Overview, Notifications center, DATA, Webex experience, Analytics, Troubleshooting, and Reports. The main content area is titled 'Meetings' and features three tabs: Sites, Settings (selected), and Templates. Under the 'Settings' tab, the 'Internal Webex Meetings' section is active, showing 'Internal meetings' settings. A dropdown menu is set to 'Allow external users to join from my organizations approved email domains'. A toggle switch is turned on for 'Apply these settings to Personal Room Meetings only'. Below this, there is a list of 'Add approved email domain' entries: 'abc.com' and 'xyz.com', each with a trash icon for deletion. A tooltip points to the toggle switch, stating: 'This setting applies to Personal Room Meetings only. Any external user can join scheduled meetings in your organization.'

webex Control Hub

Meetings

Sites Settings Templates

Internal Webex Meetings Internal meetings

These settings apply to meetings held in your organization's sites (Control Hub managed).

Allow external users to join from my organizations approved email domains

☒ Apply these settings to Personal Room Meetings only ⓘ

Add approved email domain

Email domain

abc.com

xyz.com

BRKCOL-2876

This setting applies to Personal Room Meetings only. Any external user can join scheduled meetings in your organization.

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

The screenshot displays the 'webex Control Hub' interface. On the left, a sidebar lists 'SERVICES' including Updates & Migrations, Messaging, Meeting (highlighted), Calling, Connected UC, and Hybrid. The main content area is titled 'Meeting' and shows 'External Webex Meetings' settings. A dropdown menu is set to 'Allow users to join all external meetings'. Below this, settings are organized into sections: 'Collaboration tools' (Annotation, Polling, Q&A), 'In meeting' (Chat, Closed captioning, File transfer, Participant list, Take presenter, Webex Assistant), 'Recording' (Cloud recording, Local recording), 'Remote control' (Enable remote control, Application remote control, Desktop remote control, Web browser remote control), 'Sharing' (Enable sharing, Application sharing, Desktop sharing, Doc and presentation sharing, Whiteboard, Web browser sharing), and 'Video' (Turn on video, Standard definition (360p), High definition (720p)). Each setting is accompanied by a toggle switch or checkbox.

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

The screenshot displays the Webex Control Hub interface. On the left is a sidebar with navigation options: SERVICES, Updates & Migrations, Messaging, Meeting (highlighted), Calling, Connected UC, and Hybrid. The main content area is titled 'Meeting: Disable Recording' and shows 'No Recording : Int & Ext · Rank 3' and '1 group'. Below this are tabs for 'Settings' and 'Applied groups'. The settings are organized into several sections: 'Collaboration tools' (Annotation, Polling, Q&A), 'Remote control' (Enable remote control, Application remote control, Desktop remote control, Web browser remote control), 'In meeting' (Chat, Closed captioning, File transfer, Participant list, Take presenter, Webex Assistant), 'Sharing' (Enable sharing, Application sharing, Desktop sharing, Doc and presentation sharing, Whiteboard, Web browser sharing), 'Recording' (Cloud recording, Local recording), and 'Video' (Turn on video, Standard definition (360p), High definition (720p)). Each feature has a toggle switch or checkbox to enable or disable it.

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

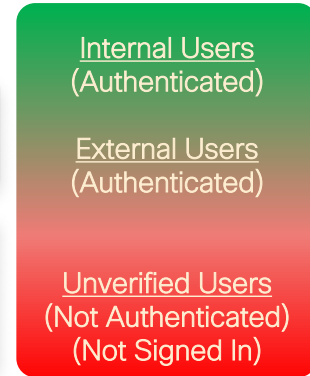
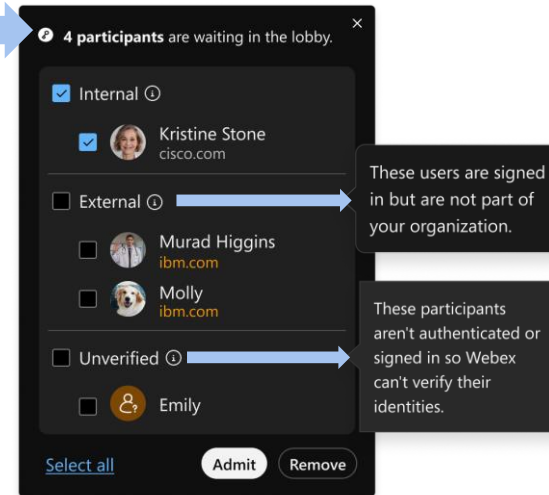
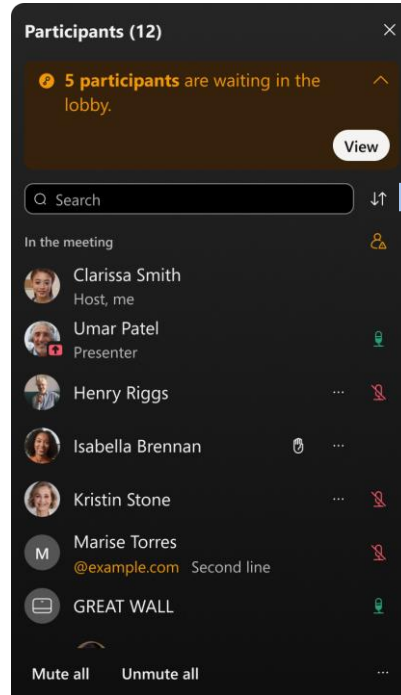
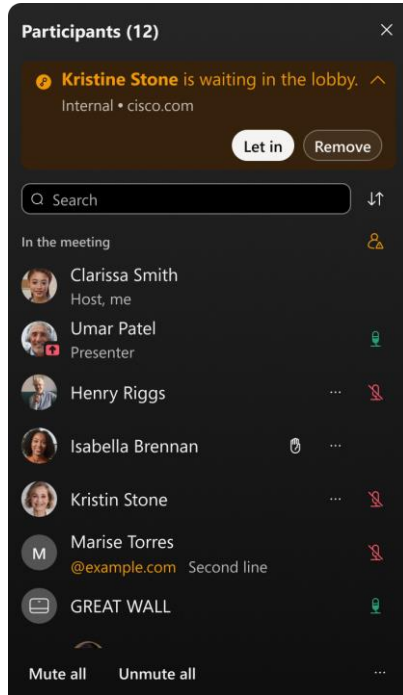
- Scheduled Meetings : Auto Admit feature
- Personal Meeting Rooms : New Lobby Controls
- Organization/ User Group/ User :
 - External Meeting Access Controls
 - Internal Meeting Access Controls
 - External Meeting Feature Controls
 - Internal Meeting Feature Controls
- Meeting Lobby/Roster/Video : Identity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



Webex Meetings : Host Controls

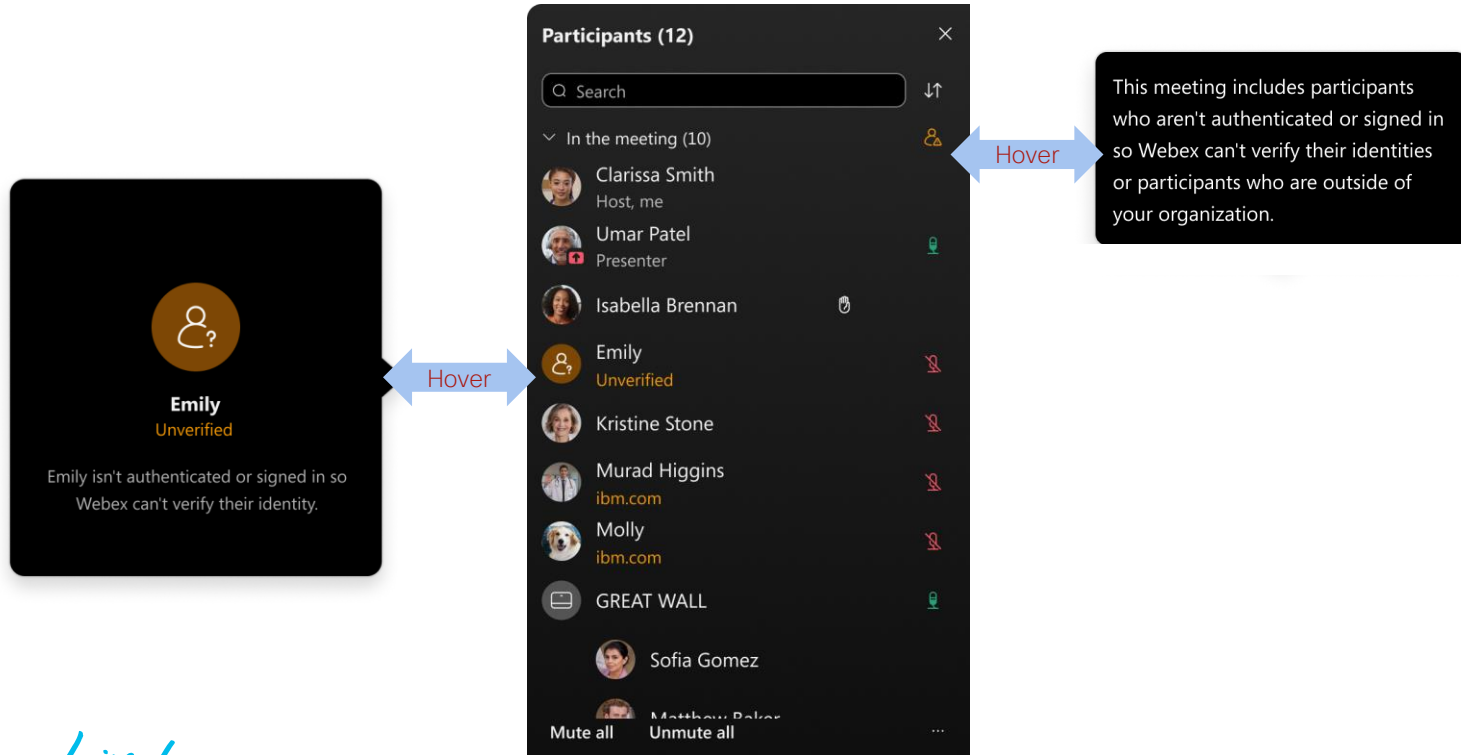
Admitting Users from the Lobby

Lobby : User Categories and User Identity information



Webex Meetings : In Meeting Participant Roster

Participant Identity Information



Video Display : User Identity information

The screenshot displays a Webex video meeting interface. The main area shows a 3x2 grid of video feeds. The top-left feed is a dark placeholder for Marise Torres (Unverified). The top-right feed shows a man in a blue shirt and headset. The middle-left feed shows a woman in a pink jacket and headset, identified as Umar Patel (Unverified). The middle-right feed is a dark placeholder for Isabelle Brennan (Unverified). The bottom-left feed shows a group of four people in a meeting room, identified as GREAT WALL. The bottom-right feed shows a man in a suit and headset. On the right side, there is a 'Participants (12)' panel with a search bar and a list of participants. At the bottom, there is a control bar with buttons for Mute, Stop video, Share, Record, and other meeting controls.

Webex Meeting info 12:40

Marise Torres (Unverified)

Umar Patel (Unverified)

Isabelle Brennan (Unverified)

GREAT WALL

Participants (12)

Search

In the meeting (10)

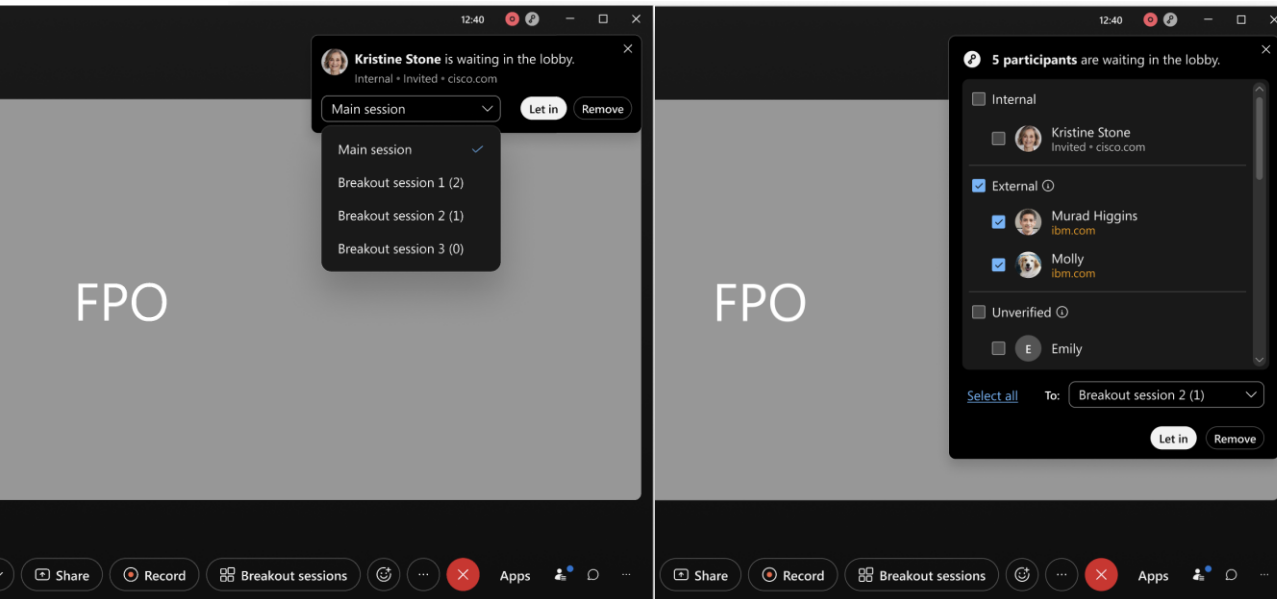
- Clarissa Smith Host, me
- Umar Patel Presenter • cisco.com
- Henry Riggs example.com
- Isabella Brennan Unverified
- Emily Wu Unverified
- Marise Torres Unverified
- GREAT WALL cisco.com
- Sofia Gomez cisco.com
- Matthew Baker cisco.com

Mute all Unmute all

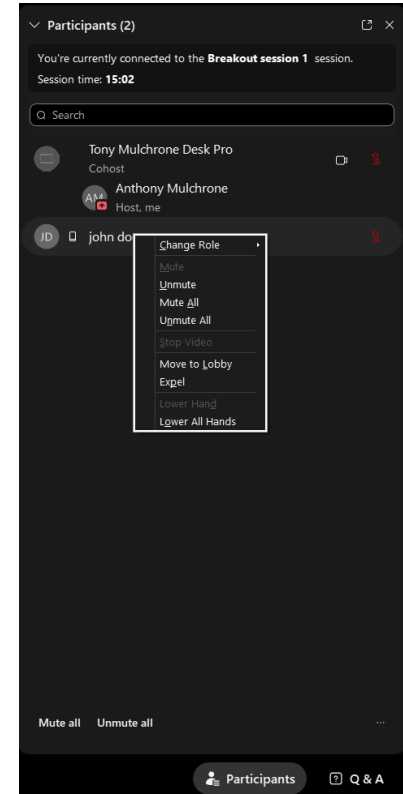
Mute Stop video Share Record Participants Chat

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.....

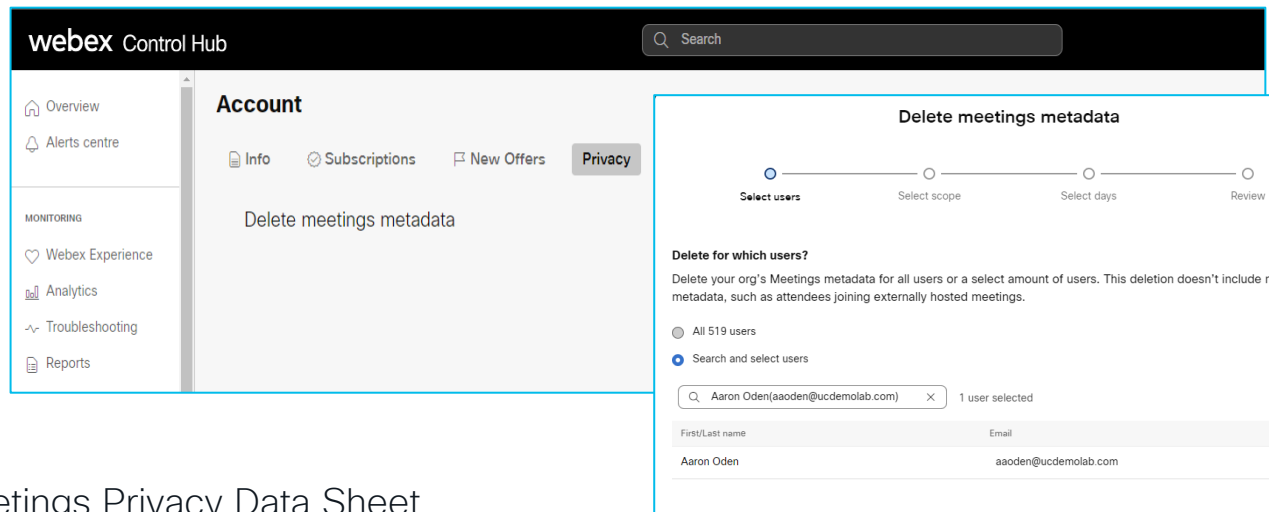
Host Name and email address

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>





The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN