cisco Live!

Let’s go

The bridge to possible

Securing Webex Meetings and avoiding meeting fraud

Privacy, Confidentiality & Security for meetings in a virtual world

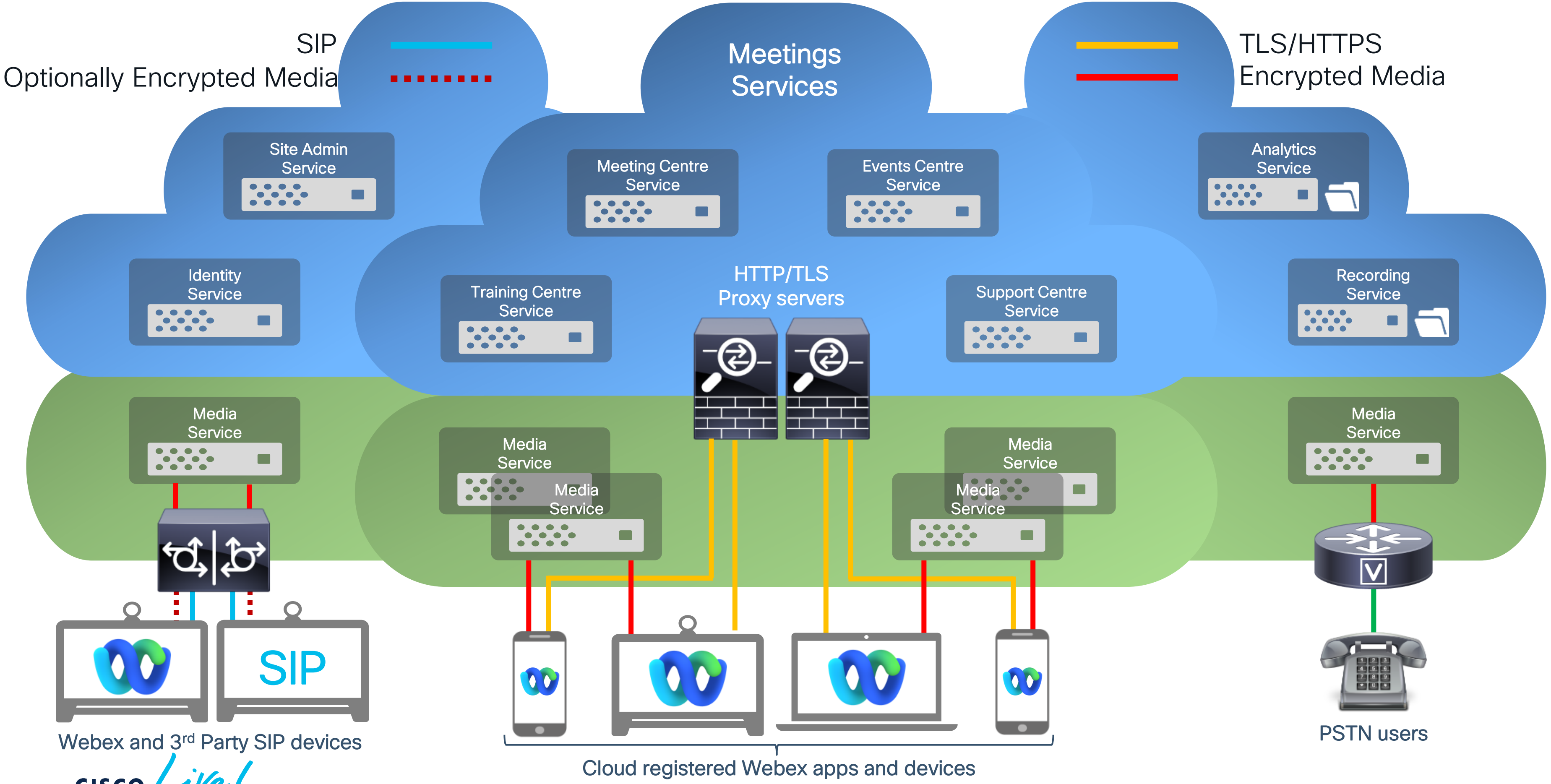
Tony Mulchrone, Principal Product Manager, Webex Security

Agenda

- Introduction
- Secure Webex platform
- Secure Webex Meeting Types : Standard, Private, End to End Encrypted
- Scheduled Webex Meetings and Webex Personal Rooms
- Securing Webex Meetings and avoiding meeting fraud
- Privacy features – Deleting meeting metadata
- E2E Encryption and E2E Identity : Technical Deep Dive

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex Meetings Architecture



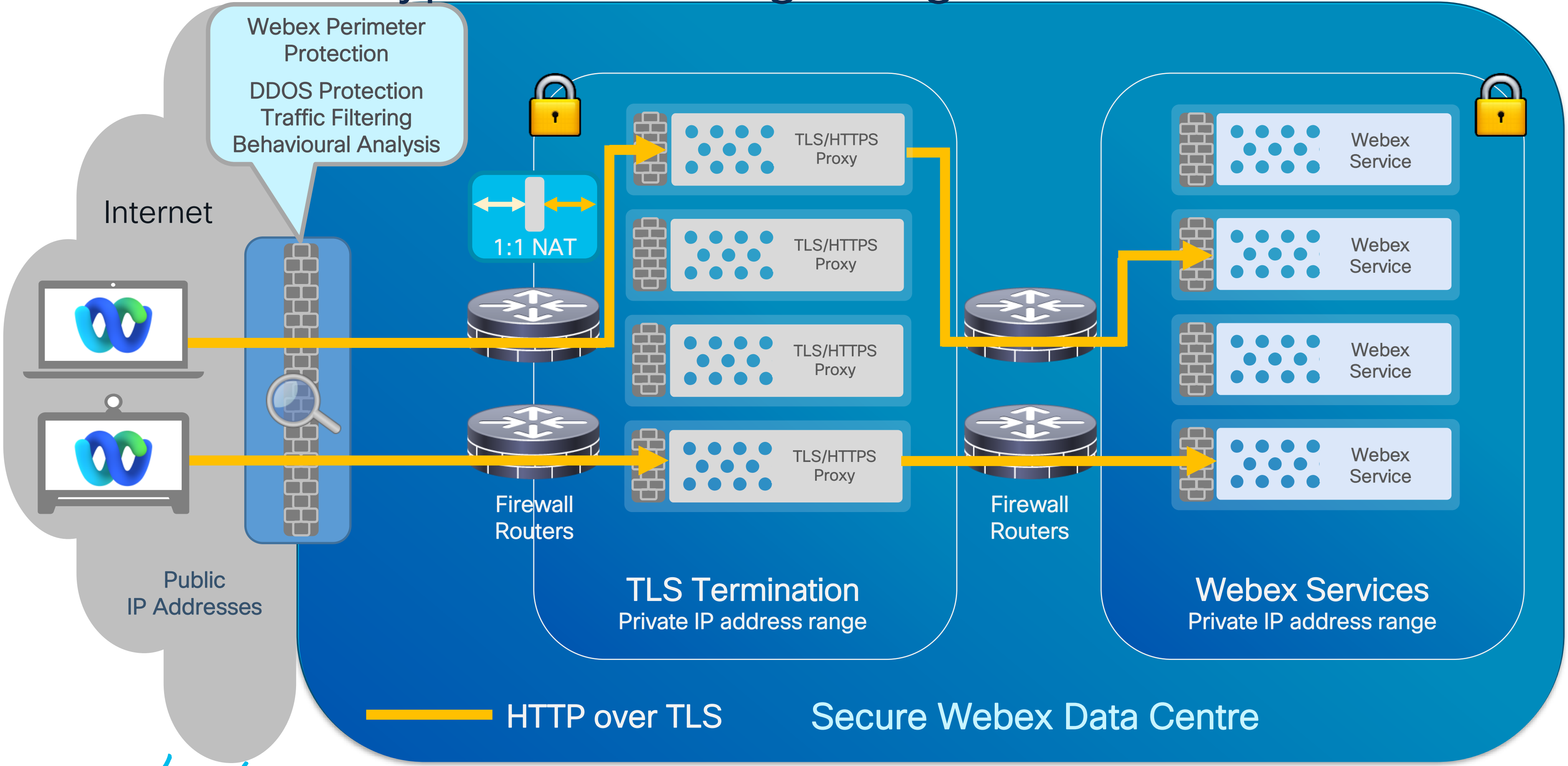
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

Webex Meetings : Secure Platform

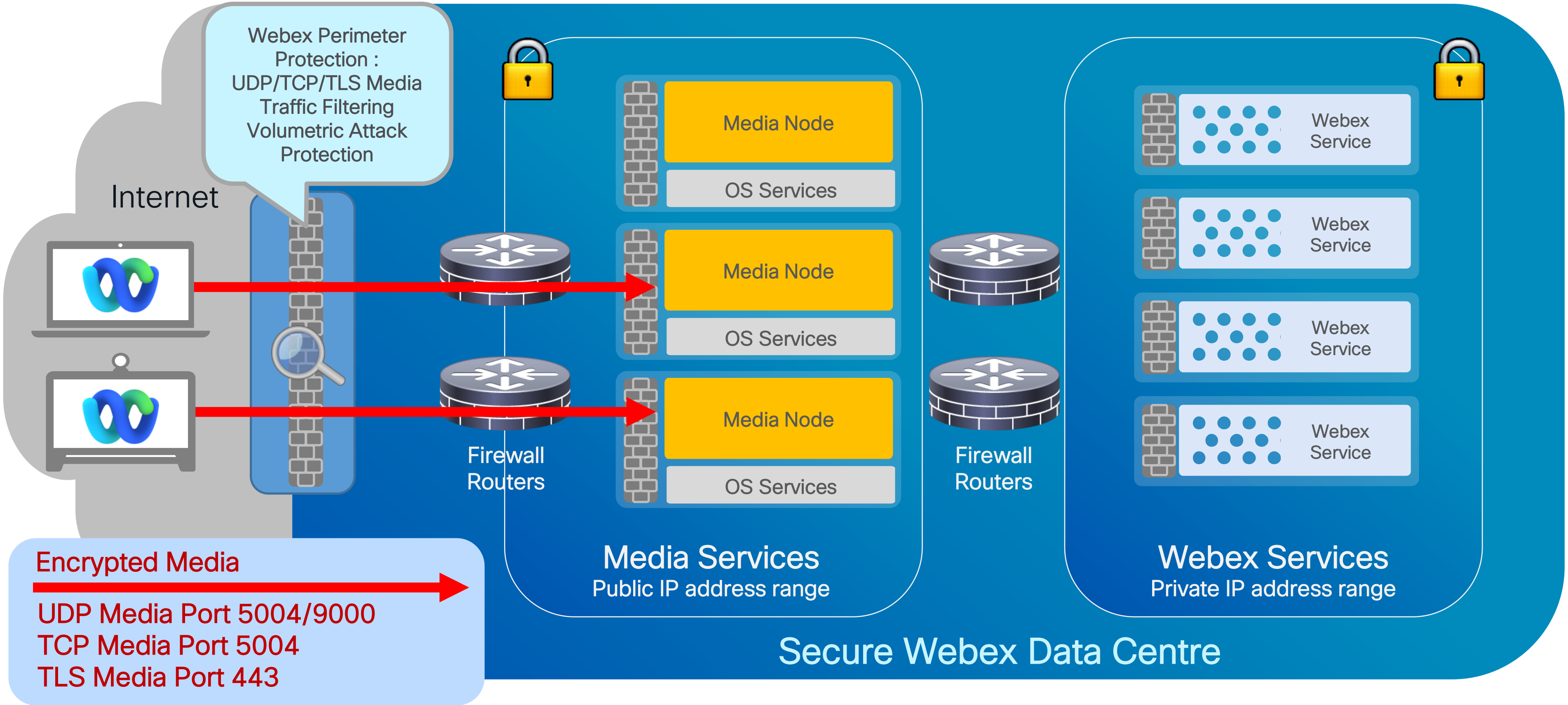
- TLS signalling
- Encrypted Media

Webex encrypted HTTP signaling – TLS/HTTPS traffic



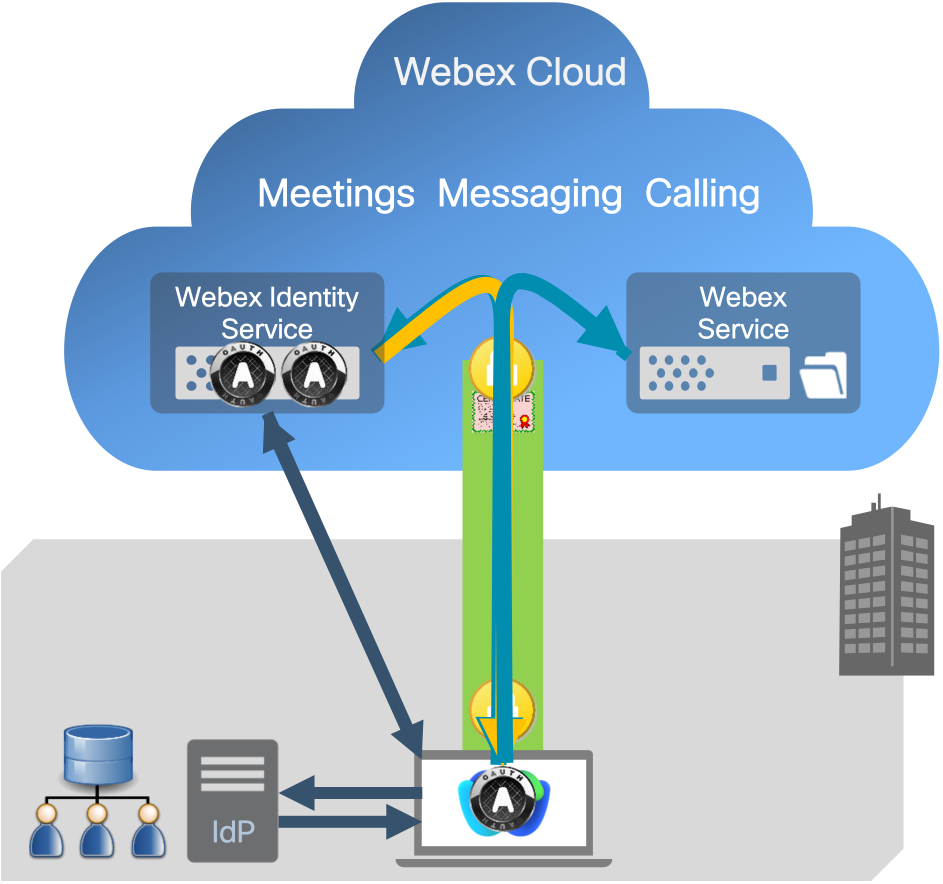
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex Media Services : Encrypted Media



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

Webex Identity – User sign in and Authorization



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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex Devices - Onboarding, Registration & Authorization

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

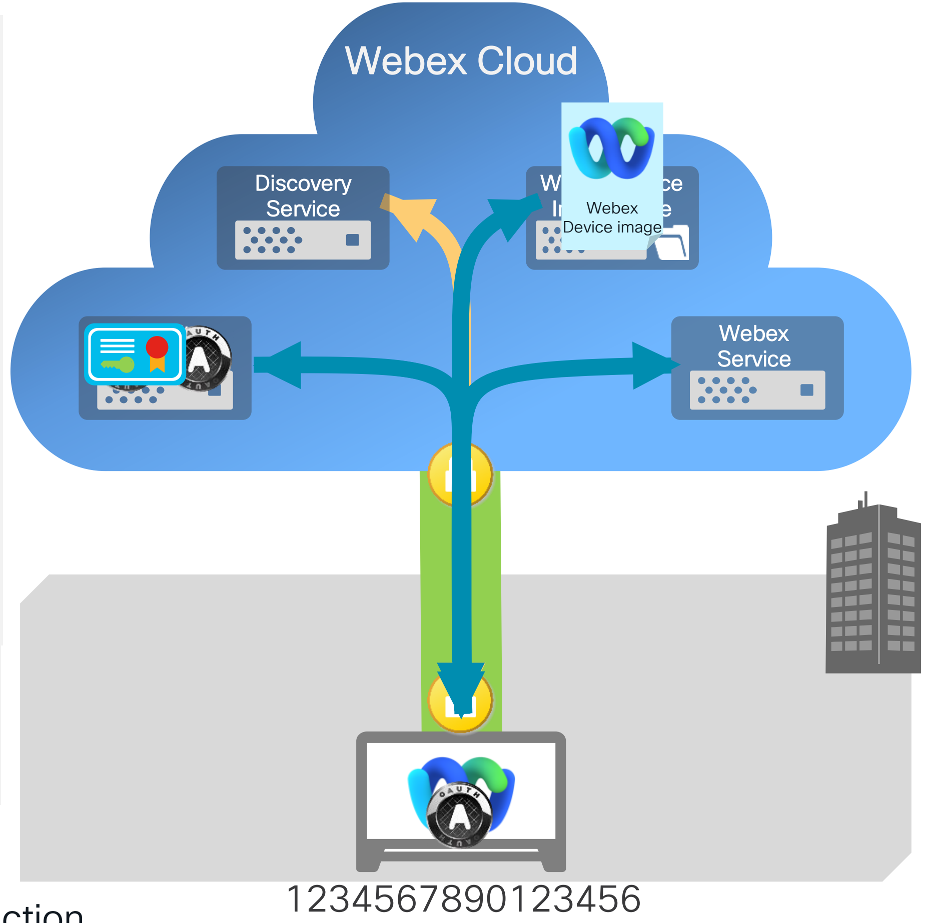
Webex Control Hub administrator generates device activation code for the device

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

Webex Meetings
Secure Meeting Types :

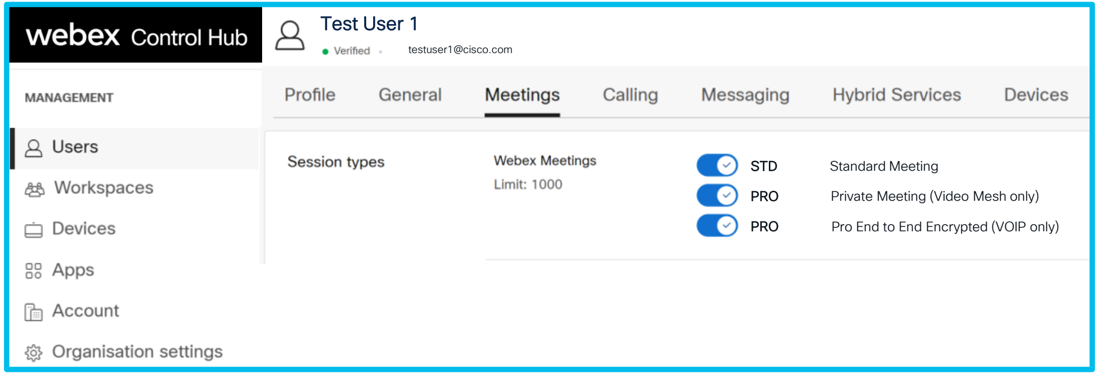
- Standard Meetings
- Private Meetings
- End to End Encrypted Meetings

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

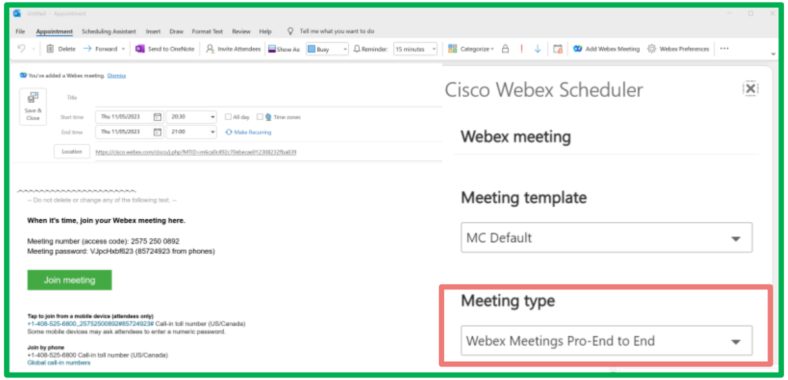


Test User 1
Verified · testuser1@cisco.com

Session types — Webex Meetings, Limit: 1000

✓	STD	Standard Meeting
✓	PRO	Private Meeting (Video Mesh only)
✓	PRO	Pro End to End Encrypted (VOIP only)

Meeting Host/ Scheduler
When scheduling a meeting via the user's webpage/ calendar/ Webex app
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



You've added a Webex meeting. Dismiss

Title:
Start time: Thu 11/05/2023 20:30 □ All day □ Time zones
End time: Thu 11/05/2023 21:00 Make Recurring
Location: https://cisco.webex.com/cisco/j.php?MTID=m6ca0c492c70ebecae012308232fba839

-- Do not delete or change any of the following text. --

When it's time, join your Webex meeting here.

Meeting number (access code): 2575 250 0892
Meeting password: VJpcHxbf623 (85724923 from phones)

Tap to join from a mobile device (attendees only)
+1-408-525-6800,,2575250892#85724923# Call-in toll number (US/Canada)
Some mobile devices may ask attendees to enter a numeric password.

Join by phone
+1-408-525-6800 Call-in toll number (US/Canada)
Global call-in numbers

Cisco Webex Scheduler

Webex meeting

Meeting template: MC Default

Meeting type: Webex Meetings Pro-End to End

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Webex Meetings

Webex Trust Webex Meetings

- Encryption and Identity

Zero Trust Webex Meetings

- End to End Encryption &
- End to End Identity

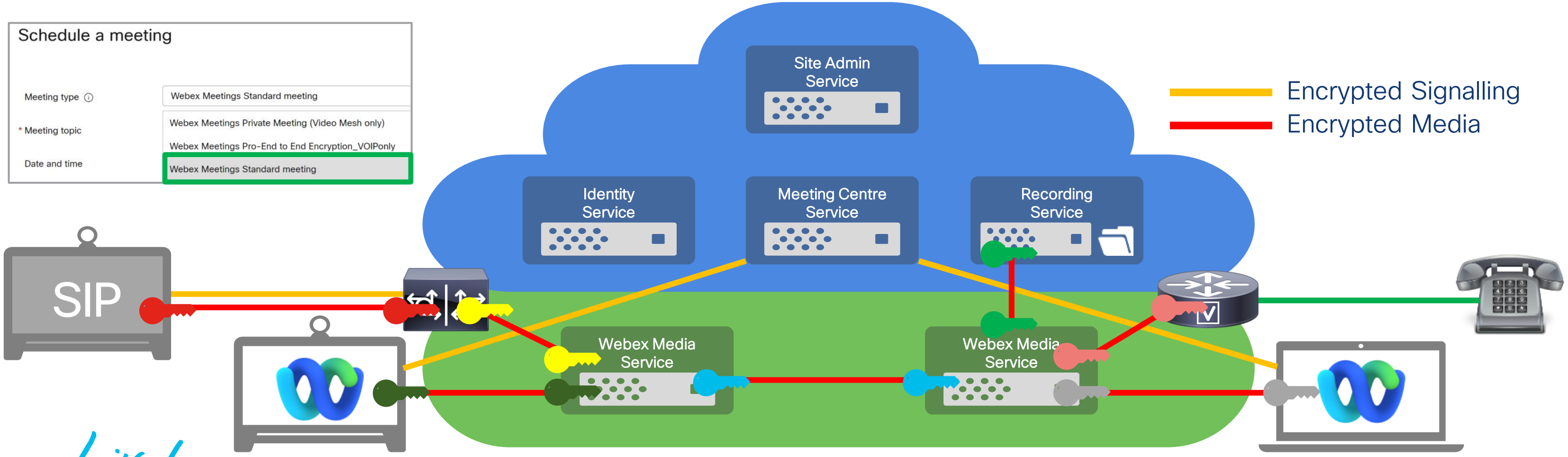
Encryption for standard Webex Meetings

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)



Schedule a meeting

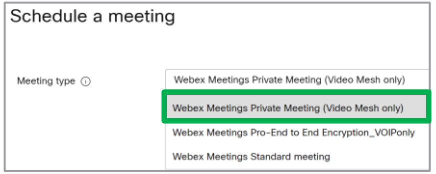
Meeting type ⓘ	Webex Meetings Standard meeting
* Meeting topic	Webex Meetings Private Meeting (Video Mesh only) Webex Meetings Pro-End to End Encryption_VOIPonly
Date and time	Webex Meetings Standard meeting

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

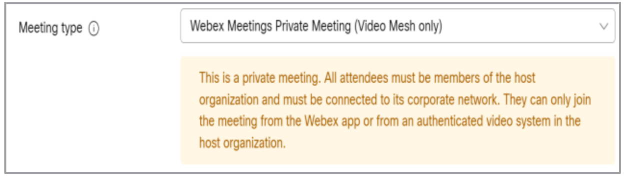
Meeting type ⓘ

- 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

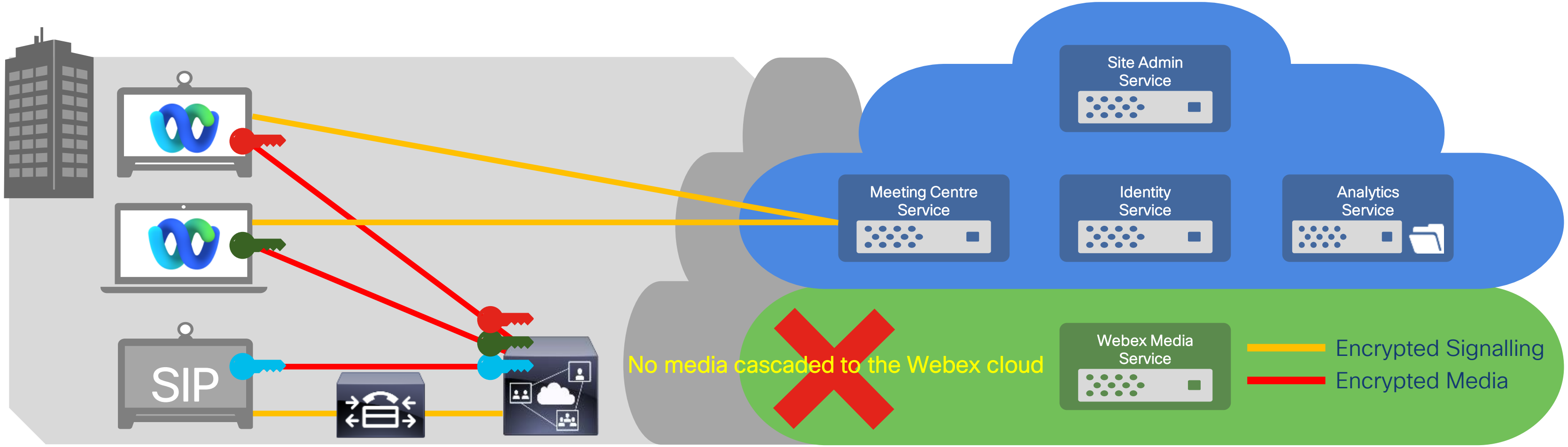
🟡 Accessibility – My org only : Cloud and SIP based users

🟡 Features - No cloud media services



Meeting type ⓘ: Webex Meetings Private Meeting (Video Mesh only)

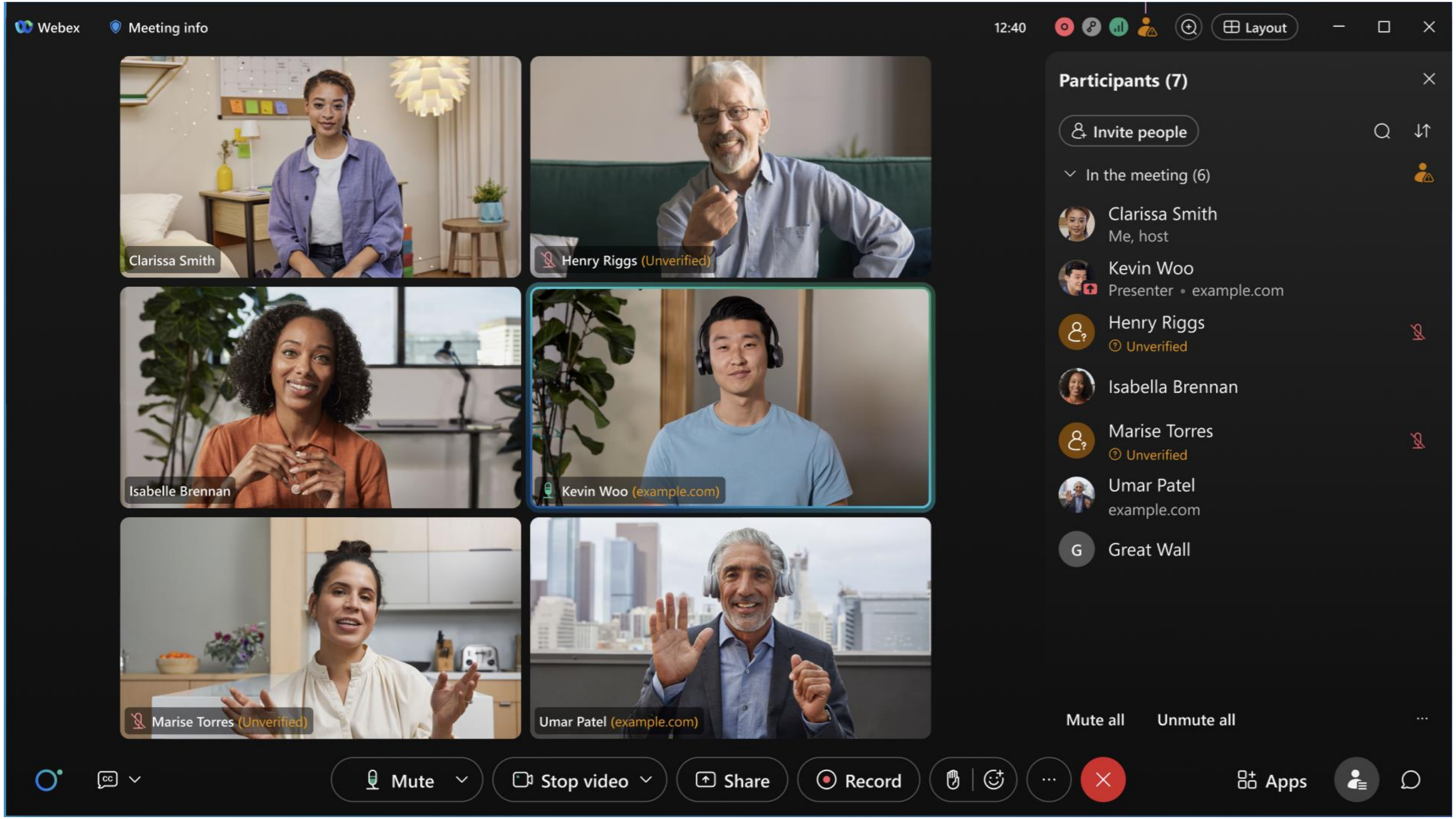
This is a private meeting. All attendees must be members of the host organization and must be connected to its corporate network. They can only join the meeting from the Webex app or from an authenticated video system in the host organization.



Video Mesh Node
Private Meeting

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Meeting Video & Roster Display : User Identity information



Participants (7)

Invite people

In the meeting (6)

Clarissa Smith
Me, host

Kevin Woo
Presenter • example.com

Henry Riggs
Unverified

Isabella Brennan

Marise Torres
Unverified

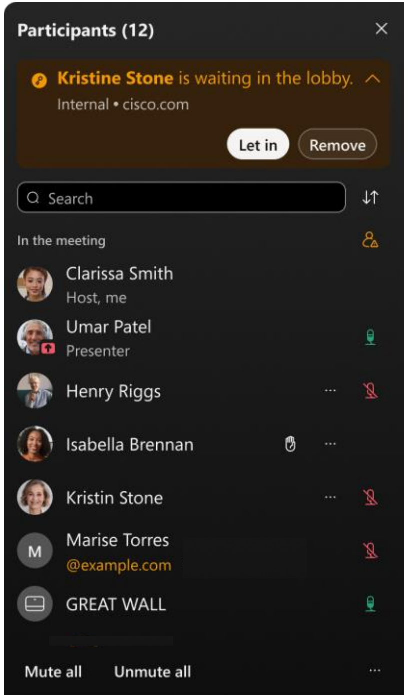
Umar Patel
example.com

Great Wall

Mute all Unmute all

Webex Meetings : Host Controls

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



Participants (12)

Kristine Stone is waiting in the lobby.
Internal • cisco.com

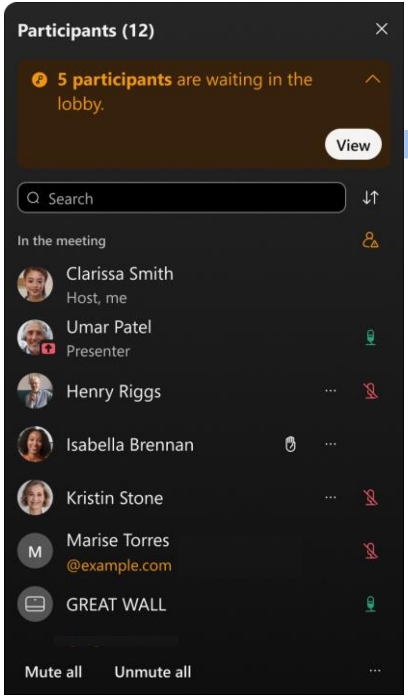
Let in | Remove

Search

In the meeting

- Clarissa Smith — Host, me
- Umar Patel — Presenter
- Henry Riggs
- Isabella Brennan
- Kristin Stone
- Marise Torres — @example.com
- GREAT WALL

Mute all | Unmute all



Participants (12)

5 participants are waiting in the lobby.

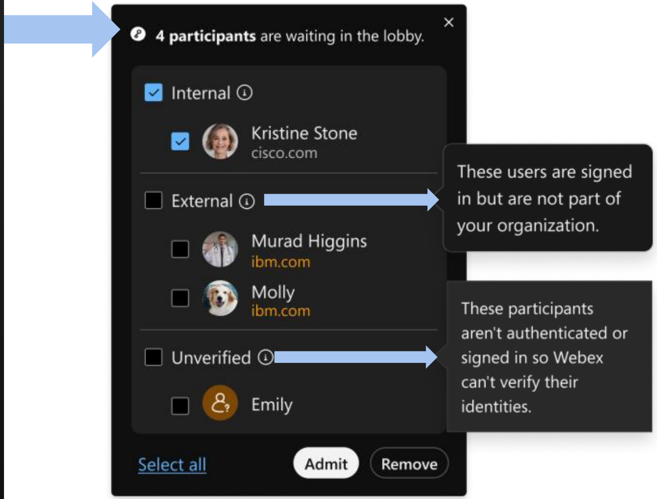
View

Search

In the meeting

- Clarissa Smith — Host, me
- Umar Patel — Presenter
- Henry Riggs
- Isabella Brennan
- Kristin Stone
- Marise Torres — @example.com
- GREAT WALL

Mute all | Unmute all



4 participants are waiting in the lobby.

☑ Internal ⓘ
- ☑ Kristine Stone — cisco.com

☐ External ⓘ
- ☐ Murad Higgins — ibm.com
- ☐ Molly — ibm.com

☐ Unverified ⓘ
- ☐ Emily

Select all | Admit | Remove

These users are signed in but are not part of your organization.

These participants aren't authenticated or signed in so Webex can't verify their identities.

Internal Users
(Authenticated)

External Users
(Authenticated)

Unverified Users
(Not Authenticated)
(Not Signed In)

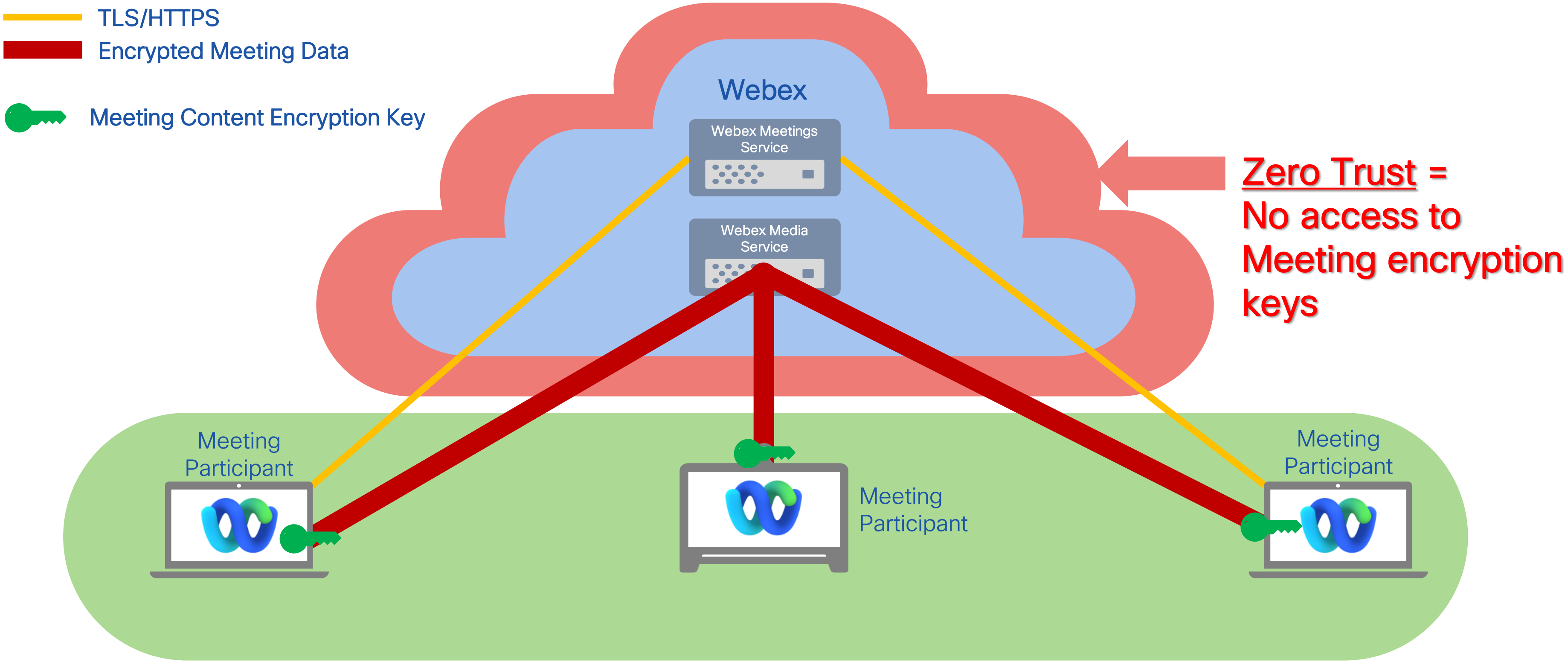
Zero Trust End to End Encryption

Question:
How do you know that your Meetings Provider does not have your meeting content encryption keys ?

Answer:

If the meeting encryption key is generated on your device and never leaves it, and this common meeting encryption key can only be generated by meeting participants

Zero Trust Security : End to End Encryption



<u>Zero Trust</u> = No access to Meeting encryption keys

Only Meeting Participants have the Meeting's content encryption key

Zero Trust End to End Identity

Question:
How do you know that your Meetings Provider cannot impersonate you, so as to get access to your meeting encryption key ?

Answer:

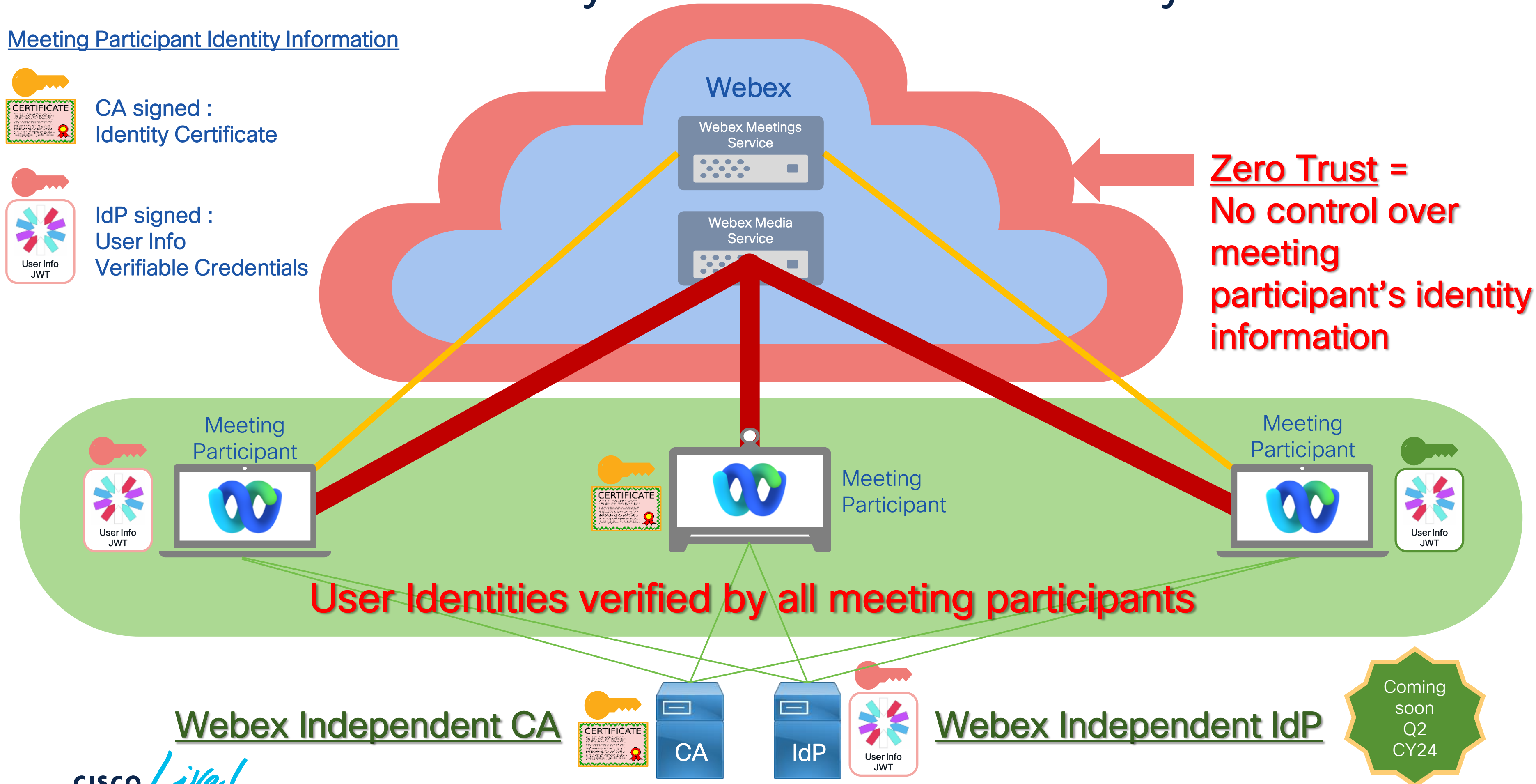
If the identity information exchanged between participants in your meeting (and used to generate the meeting encryption key) is created not by the Meetings Provider, but by an independent/ external Identity Provider and verified by each participant

Zero Trust Security : End to End Identity

Meeting Participant Identity Information

CA signed :
Identity Certificate

IdP signed :
User Info
Verifiable Credentials



Zero Trust = No control over meeting participant's identity information

User Identities verified by all meeting participants

Webex Independent CA

Webex Independent IdP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Webex Meetings

Webex Trust Webex Meetings

- Encryption and Identity

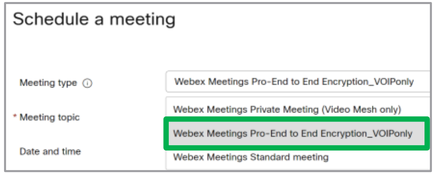
Zero Trust Webex Meetings

- End to End Encryption &
- End to End Identity

Zero Trust Security for Webex Meetings – E2E Media Encryption

MLS and SFrame operation

- 🟢 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



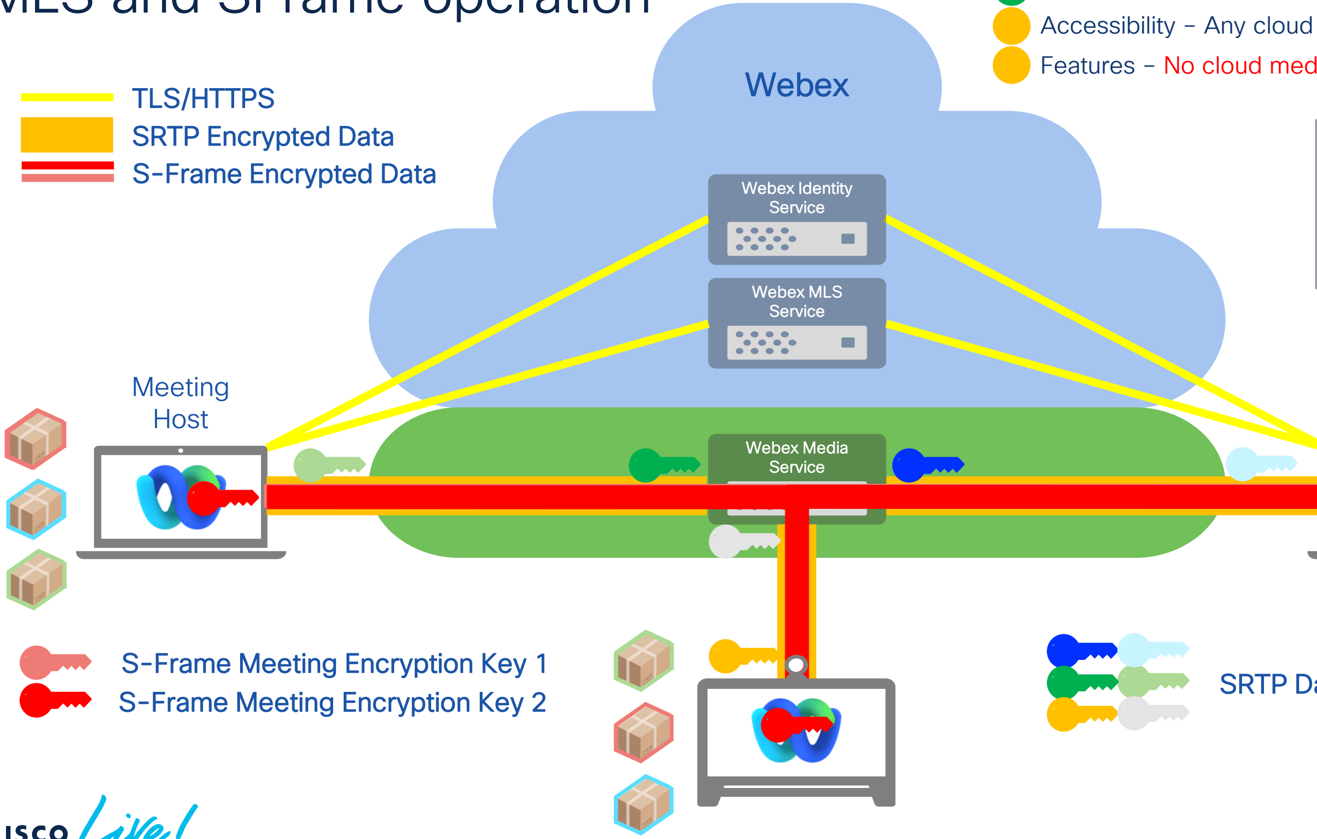
Schedule a meeting

Meeting type ⓘ: Webex Meetings Pro-End to End Encryption_VOIPonly

* Meeting topic

Date and time

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



TLS/HTTPS

SRTP Encrypted Data

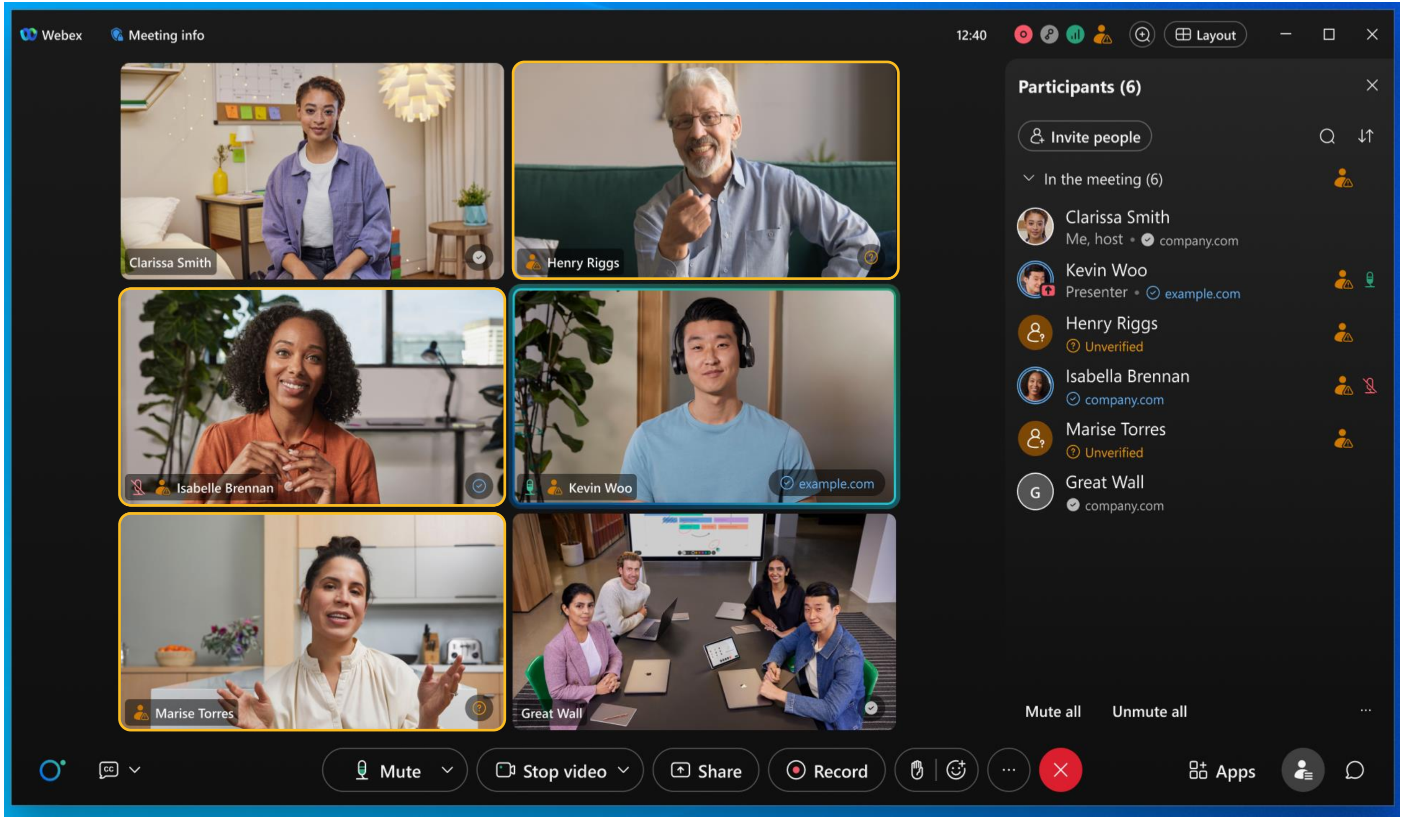
S-Frame Encrypted Data

S-Frame Meeting Encryption Key 1

S-Frame Meeting Encryption Key 2

SRTP Data Encryption Keys

Zero Trust Security for Webex Meetings : E2E Identity Meeting Roster - User Identity details



Participants (6)

Invite people

In the meeting (6)

Clarissa Smith
Me, host • company.com

Kevin Woo
Presenter • example.com

Henry Riggs
Unverified

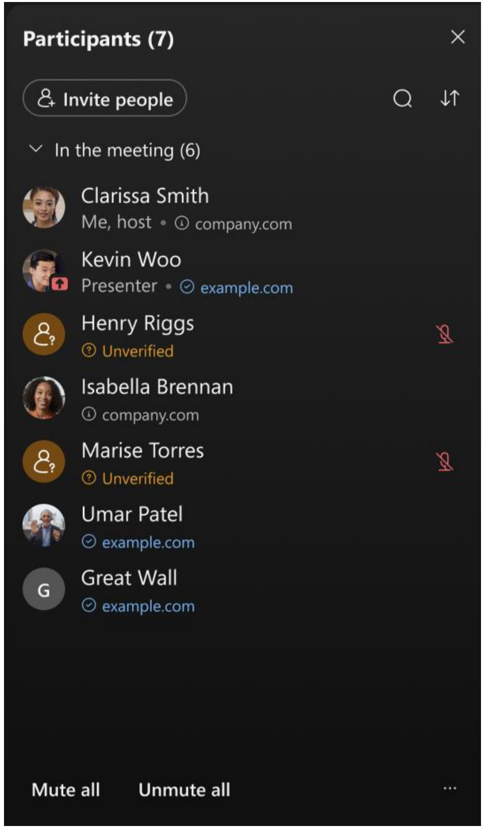
Isabella Brennan
company.com

Marise Torres
Unverified

Great Wall
company.com

Mute all Unmute all

Zero Trust Security for Webex Meetings : E2E Identity Meeting Roster – User Identity details



Participants (7)

Invite people

In the meeting (6)

Clarissa Smith
Me, host • ⓘ company.com

Kevin Woo
Presenter • ✓ example.com

Henry Riggs
? Unverified

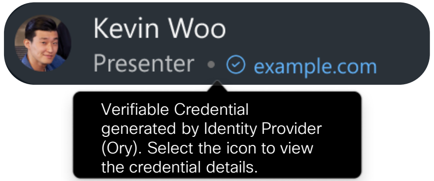
Isabella Brennan
ⓘ company.com

Marise Torres
? Unverified

Umar Patel
✓ example.com

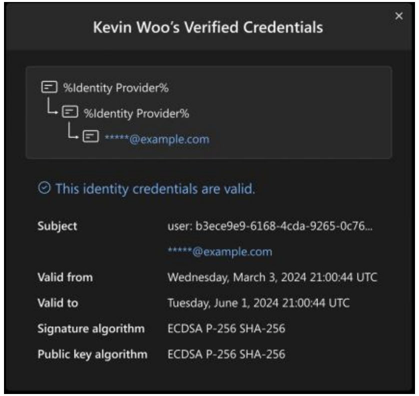
Great Wall
✓ example.com

Mute all Unmute all



Kevin Woo
Presenter • ✓ example.com

Verifiable Credential generated by Identity Provider (Ory). Select the icon to view the credential details.

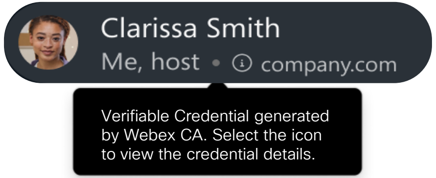


Kevin Woo's Verified Credentials

%Identity Provider%
└ %Identity Provider%
  └ *****@example.com

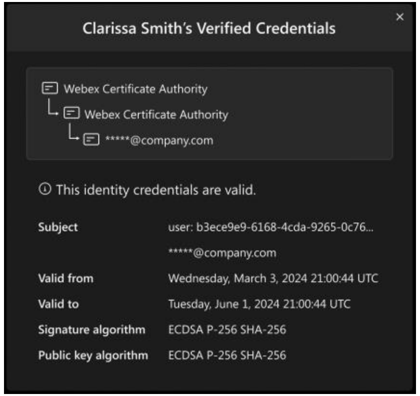
✓ This identity credentials are valid.

Subject	user: b3ece9e9-6168-4cda-9265-0c76... *****@example.com
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256



Clarissa Smith
Me, host • ⓘ company.com

Verifiable Credential generated by Webex CA. Select the icon to view the credential details.



Clarissa Smith's Verified Credentials

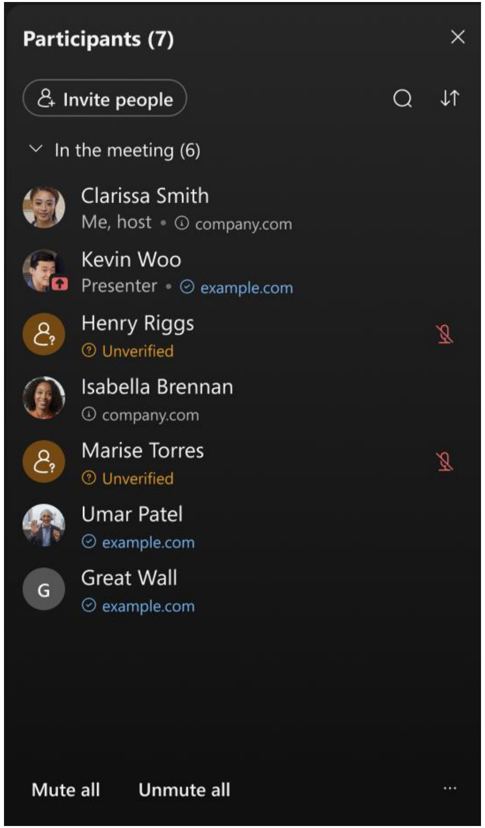
Webex Certificate Authority
└ Webex Certificate Authority
  └ *****@company.com

ⓘ This identity credentials are valid.

Subject	user: b3ece9e9-6168-4cda-9265-0c76... *****@company.com
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security for Webex Meetings : E2E Identity Meeting Roster - User Identity details



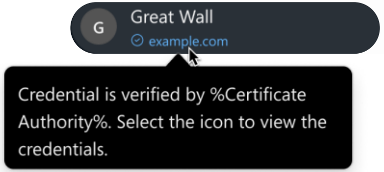
Participants (7)

Invite people

In the meeting (6)

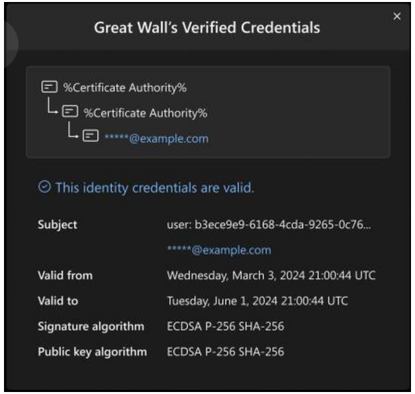
- Clarissa Smith — Me, host • ⓘ company.com
- Kevin Woo — Presenter • ✓ example.com
- Henry Riggs — ⓘ Unverified
- Isabella Brennan — ⓘ company.com
- Marise Torres — ⓘ Unverified
- Umar Patel — ✓ example.com
- Great Wall — ✓ example.com

Mute all   Unmute all   ...



Great Wall
✓ example.com

Credential is verified by %Certificate Authority%. Select the icon to view the credentials.

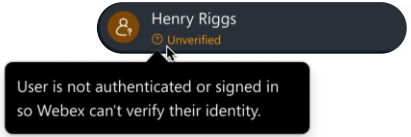


Great Wall's Verified Credentials

```
%Certificate Authority%
└ %Certificate Authority%
  └ *****@example.com
```

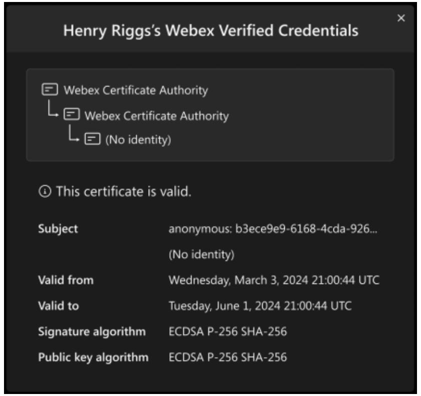
✓ This identity credentials are valid.

Subject	user: b3ece9e9-6168-4cda-9265-0c76... *****@example.com
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256



Henry Riggs
ⓘ Unverified

User is not authenticated or signed in so Webex can't verify their identity.



Henry Riggs's Webex Verified Credentials

```
Webex Certificate Authority
└ Webex Certificate Authority
  └ (No identity)
```

ⓘ This certificate is valid.

Subject	anonymous: b3ece9e9-6168-4cda-926... (No identity)
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256

Webex Meetings :

Scheduled Meetings and Personal Room Meetings

Scheduled Webex Meetings

Most secure and preferred meeting type

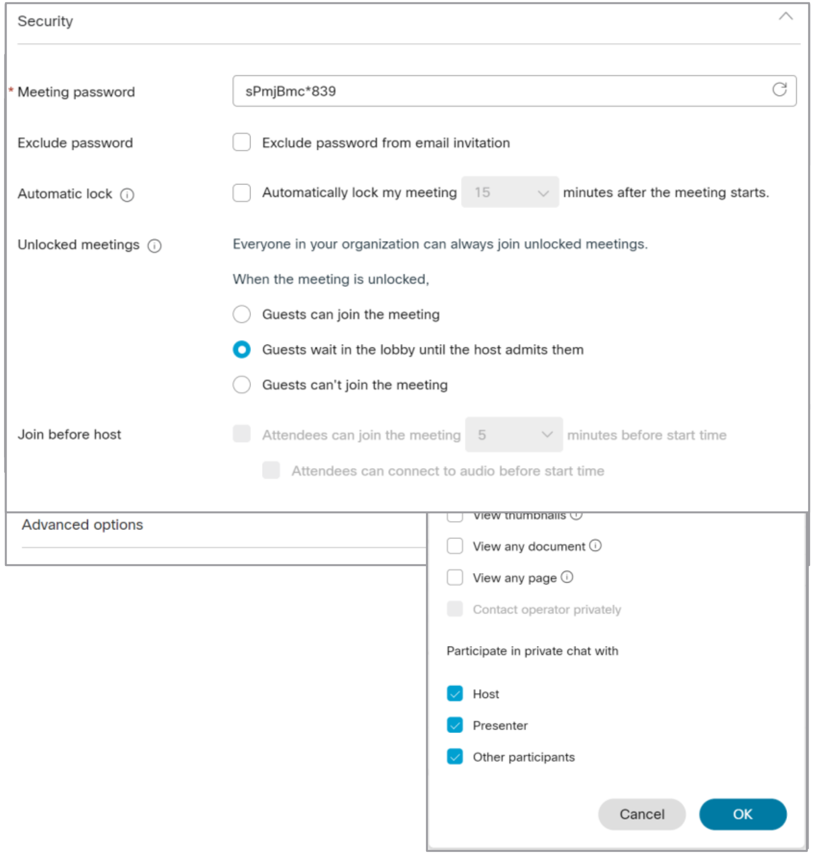
- Multiple meeting types available
- One time meeting or recurring

- 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



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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

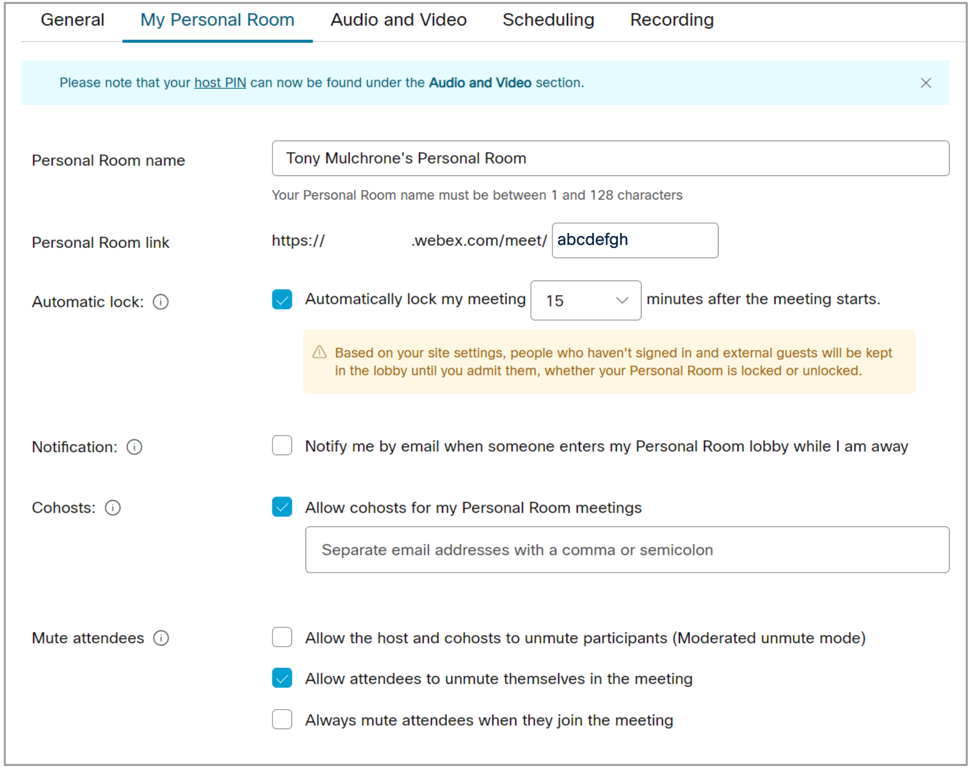
Webex Personal Room Meetings

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



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

Administrator and Meeting Host - Security documents

Webex best practices for secure meetings: Control Hub

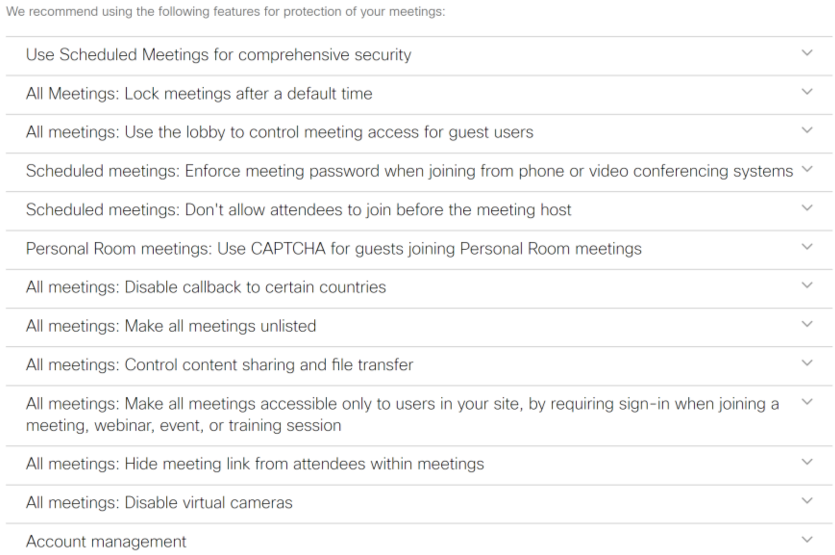
https://help.webex.com/en-us/article/ov50hy/Webex-best-practices-for-secure-meetings:-Control-Hub

Webex best practices for secure meetings: Site Administration

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

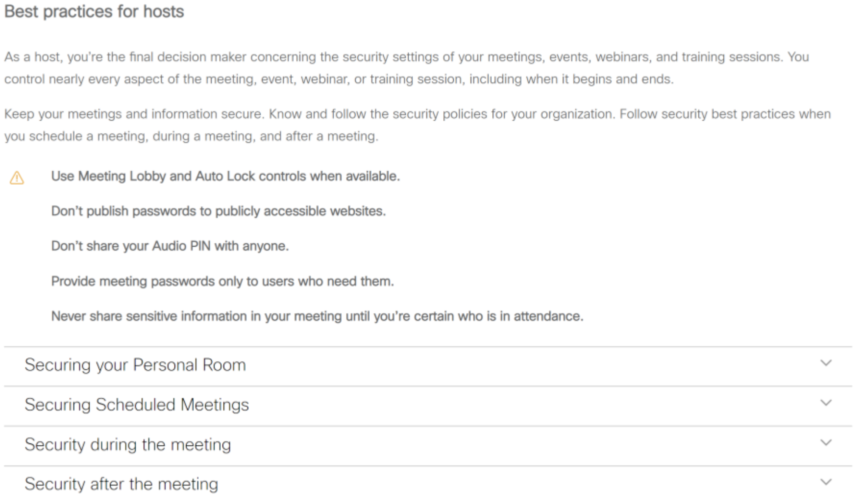
Webex best practices for secure meetings: hosts

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



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



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

Deepfake and other exploits...

Avoiding fraud and unwanted attendees

Webex features for user screening & controlled access to meetings

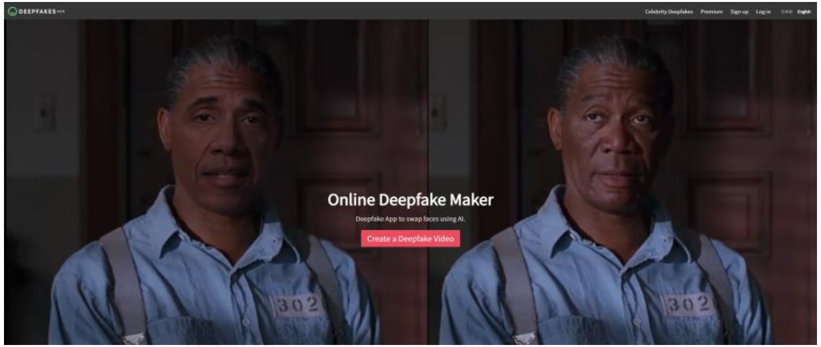
Deepfake and online meetings

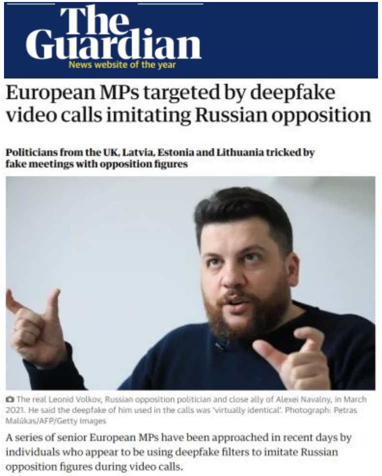
- Deepfake software is freely available today
- Deepfake exploits are usually sophisticated attacks or doctored pre-recorded video
- Instances of meetings with fraudulent users using deepfake are relatively small today, but there have been several significant cases

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.....





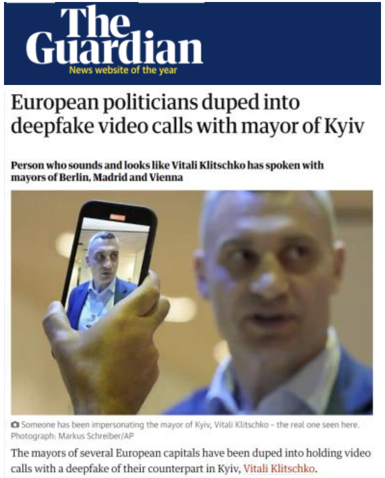
The Guardian
News website of the year

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.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

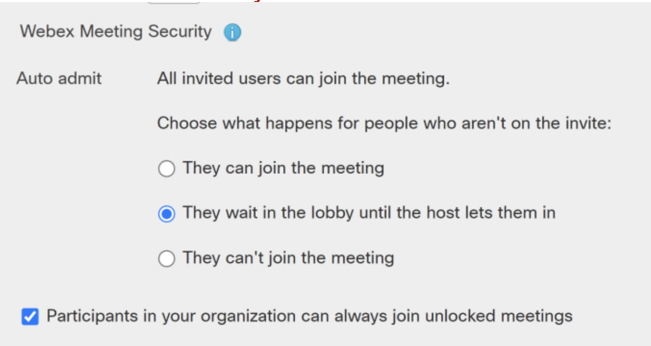
New Webex Meetings Security features

- 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

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:

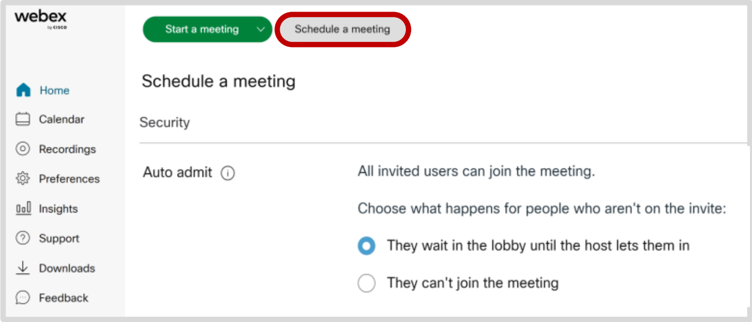
○ They can join the meeting

● 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



Schedule a meeting

Security

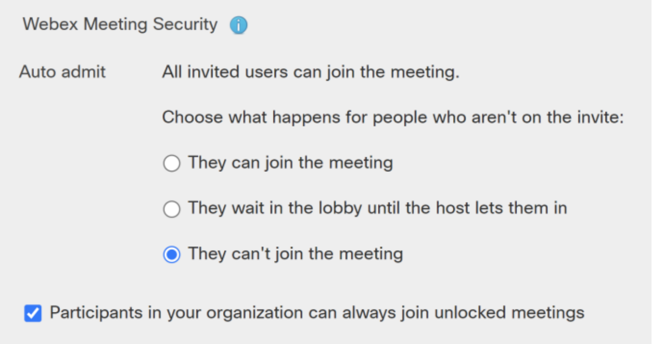
Auto admit — All invited users can join the meeting.

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:

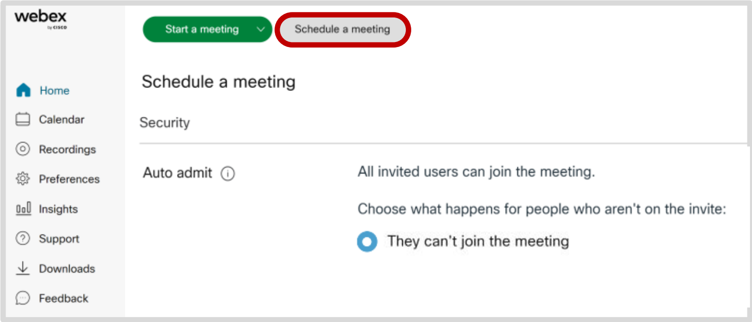
○ They can join the meeting

○ 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



Schedule a meeting

Security

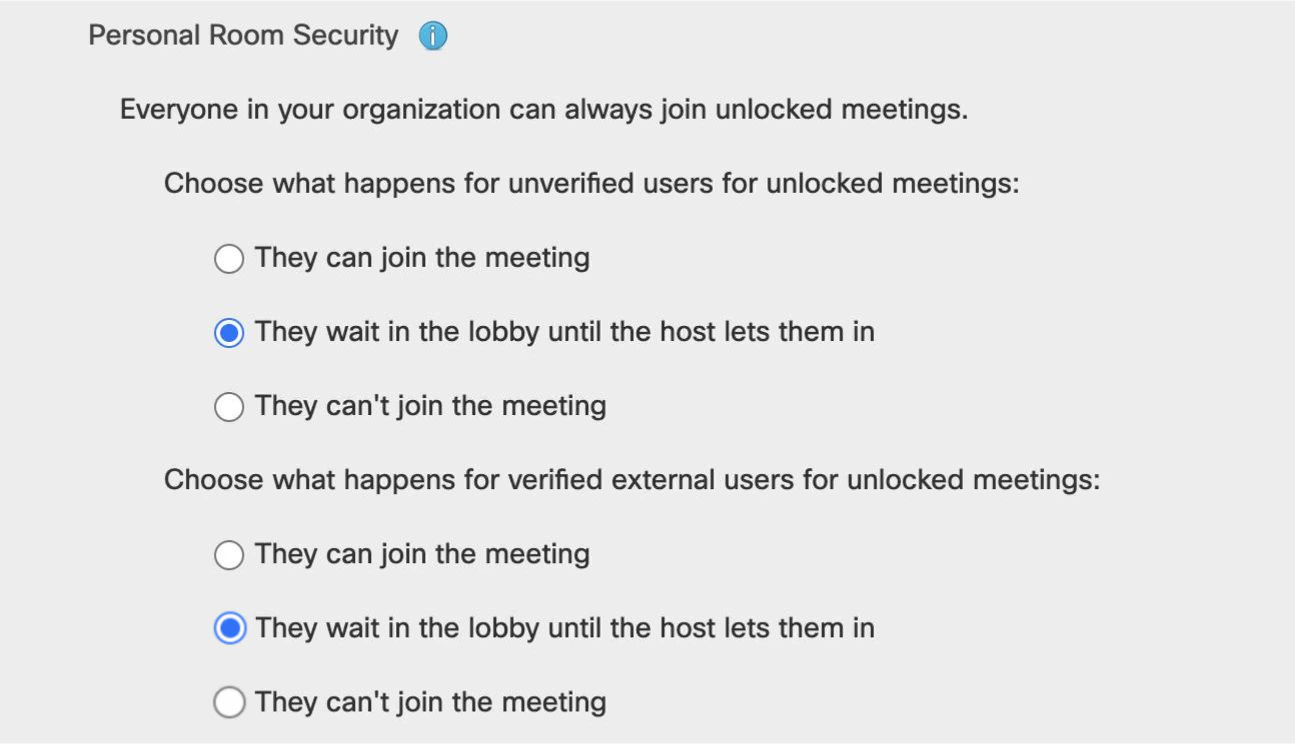
Auto admit — All invited users can join the meeting.

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

Previously :
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.

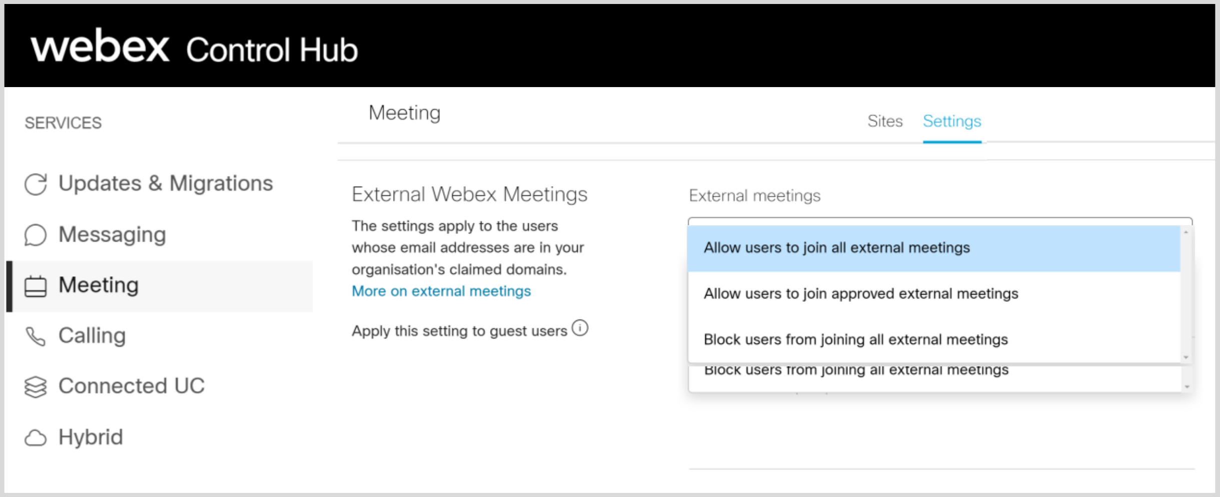
Allows administrators to apply different sets of controls for these groups of users, to reduce lobby bloat and meeting fraud

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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



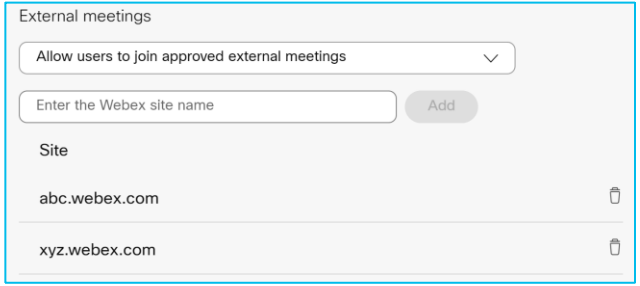
External Webex Meetings

The settings apply to the users whose email addresses are in your organisation's claimed domains.
More on external meetings

Apply this setting to guest users ⓘ

External meetings

- Allow users to join all external meetings
- Allow users to join approved external meetings
- Block users from joining all external meetings


External meetings: Allow users to join approved external meetings

Site
abc.webex.com
xyz.webex.com

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

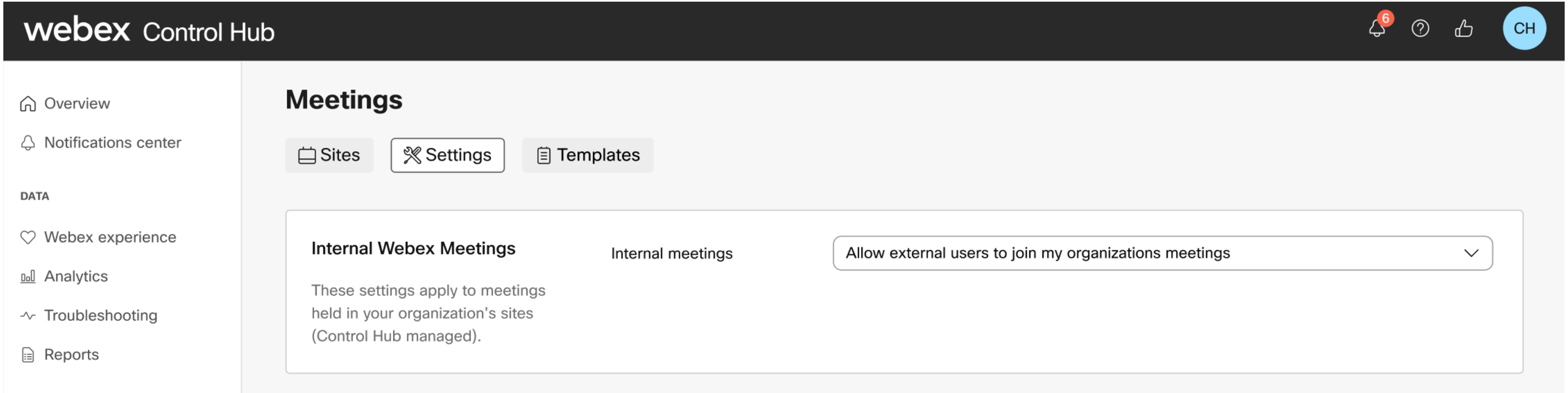
These controls can be applied to :

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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)



Meetings

Internal Webex Meetings

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

Internal meetings: Allow external users to join my organizations meetings

These controls can be applied to :

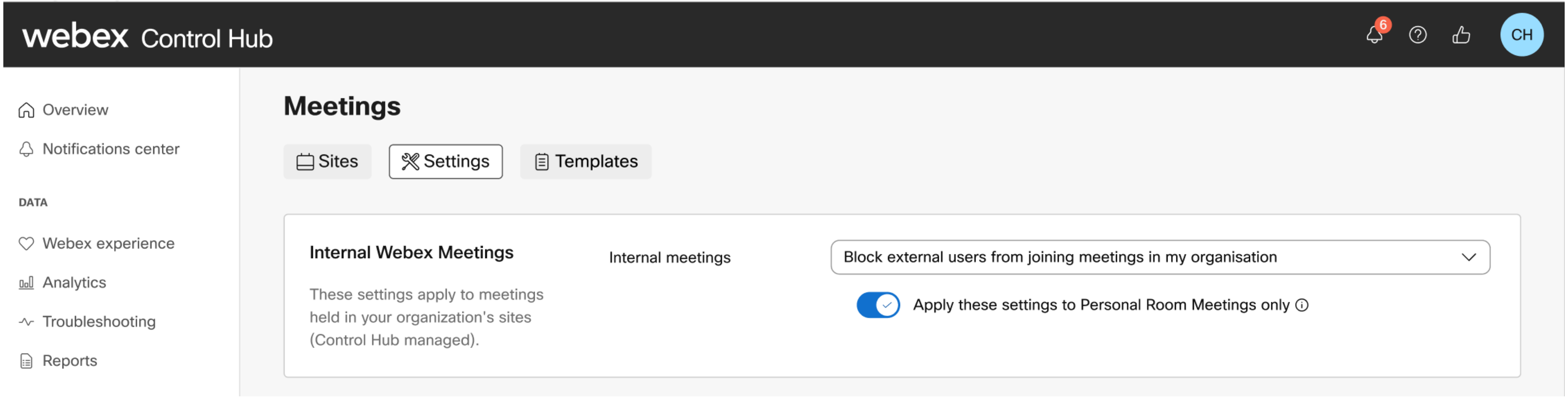
- All users in the organization
- Groups of users – using Templates applied to user groups
- Individual users – user profile

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



Internal Webex Meetings

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

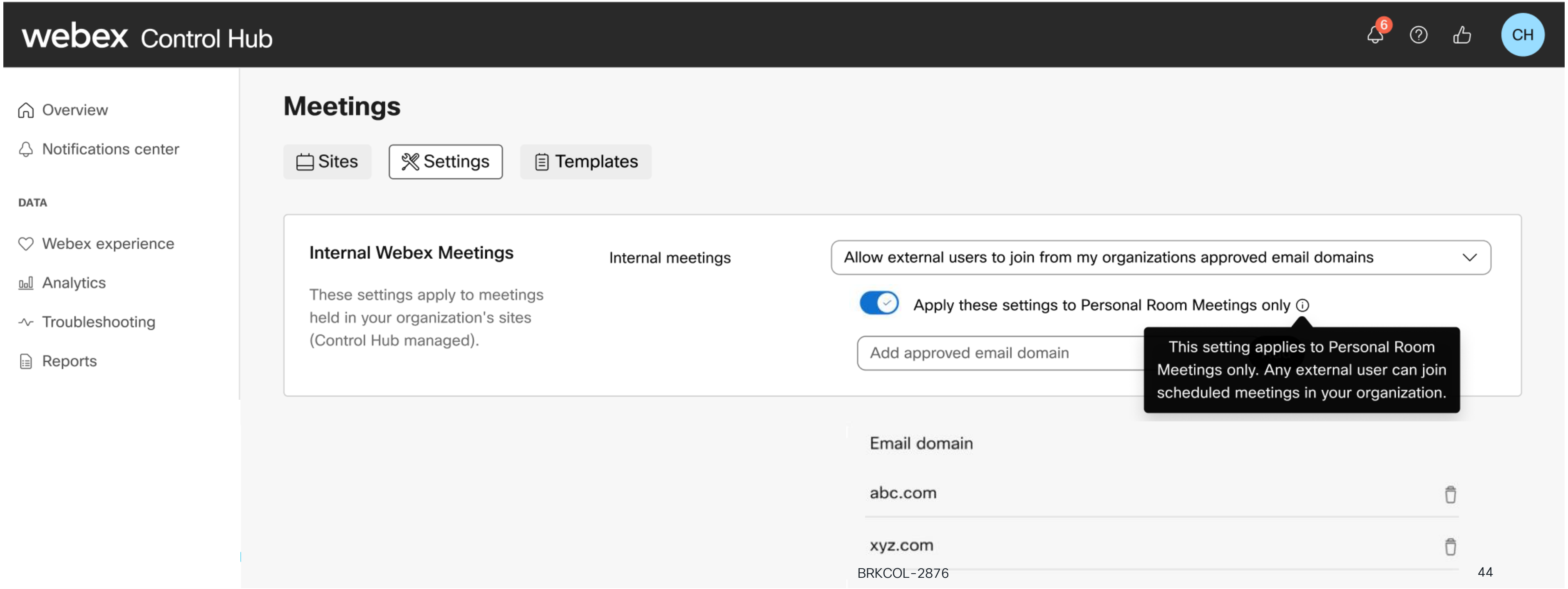
Internal meetings: Block external users from joining meetings in my organisation

Apply these settings to Personal Room Meetings only (on)

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



Meetings

Internal Webex Meetings

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

Internal meetings: Allow external users to join from my organizations approved email domains

Apply these settings to Personal Room Meetings only

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

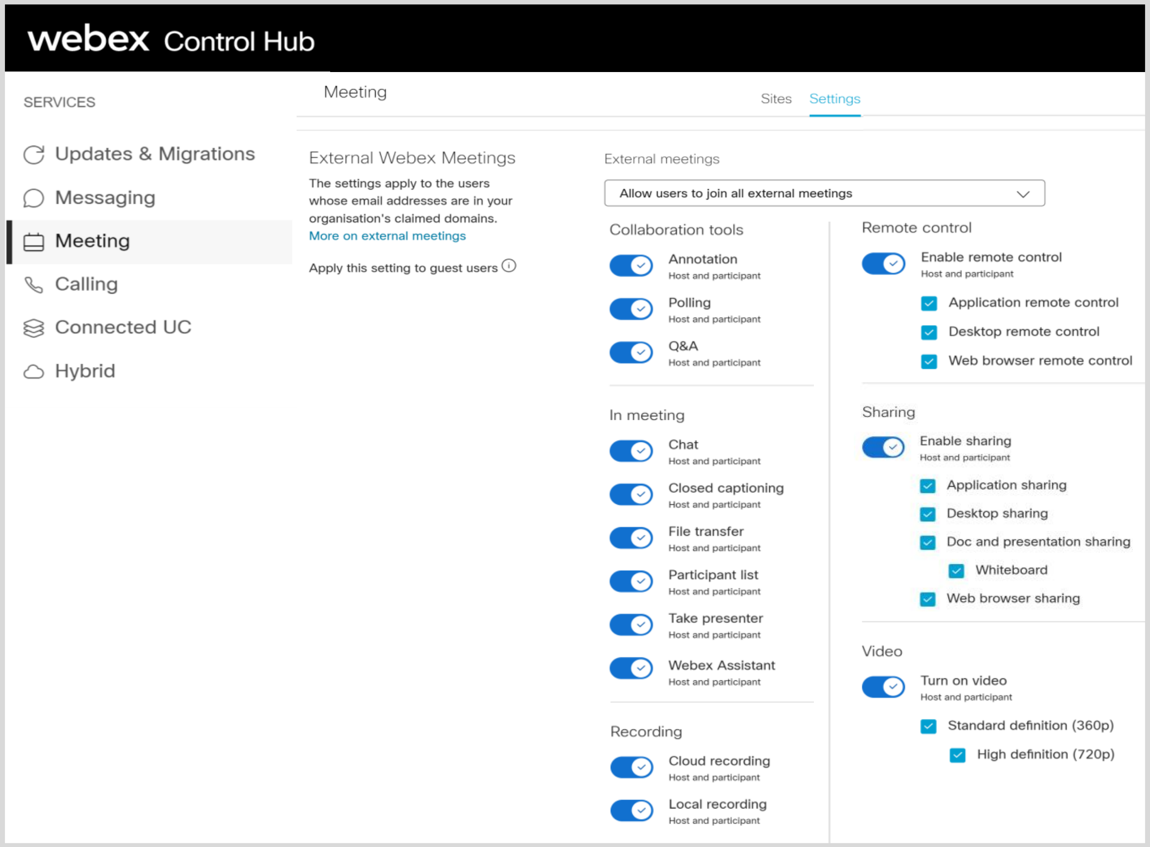
Add approved email domain

Email domain
abc.com
xyz.com

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

Feature Controls for External Webex Meetings



External Webex Meetings

The settings apply to the users whose email addresses are in your organisation's claimed domains.
More on external meetings

Apply this setting to guest users ⓘ

External meetings: Allow users to join all external meetings

Collaboration tools
- ✓ Annotation — Host and participant
- ✓ Polling — Host and participant
- ✓ Q&A — Host and participant

In meeting
- ✓ Chat — Host and participant
- ✓ Closed captioning — Host and participant
- ✓ File transfer — Host and participant
- ✓ Participant list — Host and participant
- ✓ Take presenter — Host and participant
- ✓ Webex Assistant — Host and participant

Recording
- ✓ Cloud recording — Host and participant
- ✓ Local recording — Host and participant

Remote control
- ✓ Enable remote control — Host and participant
  - ☑ Application remote control
  - ☑ Desktop remote control
  - ☑ Web browser remote control

Sharing
- ✓ Enable sharing — Host and participant
  - ☑ Application sharing
  - ☑ Desktop sharing
  - ☑ Doc and presentation sharing
    - ☑ Whiteboard
  - ☑ Web browser sharing

Video
- ✓ Turn on video — Host and participant
  - ☑ Standard definition (360p)
    - ☑ High definition (720p)

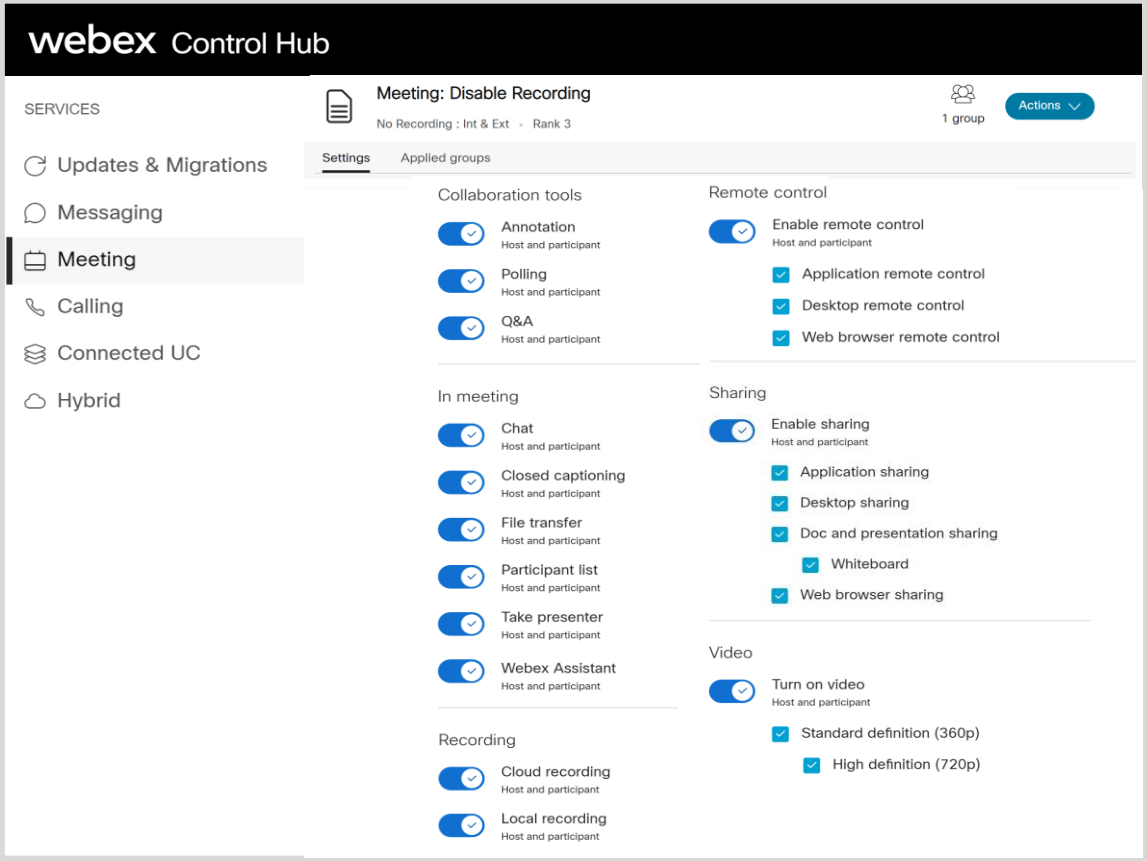
These meeting feature controls apply when users in your organization join any external Webex meeting

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Feature Controls for Internal Webex Meetings



Meeting: Disable Recording

No Recording : Int & Ext · Rank 3

Collaboration tools

- Annotation (on) – Host and participant
- Polling (on) – Host and participant
- Q&A (on) – Host and participant

In meeting

- Chat (on) – Host and participant
- Closed captioning (on) – Host and participant
- File transfer (on) – Host and participant
- Participant list (on) – Host and participant
- Take presenter (on) – Host and participant
- Webex Assistant (on) – Host and participant

Recording

- Cloud recording (on) – Host and participant
- Local recording (on) – Host and participant

Remote control

- Enable remote control (on) – Host and participant
  - ☑ Application remote control
  - ☑ Desktop remote control
  - ☑ Web browser remote control

Sharing

- Enable sharing (on) – Host and participant
  - ☑ Application sharing
  - ☑ Desktop sharing
  - ☑ Doc and presentation sharing
    - ☑ Whiteboard
  - ☑ Web browser sharing

Video

- Turn on video (on) – Host and participant
  - ☑ Standard definition (360p)
    - ☑ High definition (720p)

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

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 Features : Security

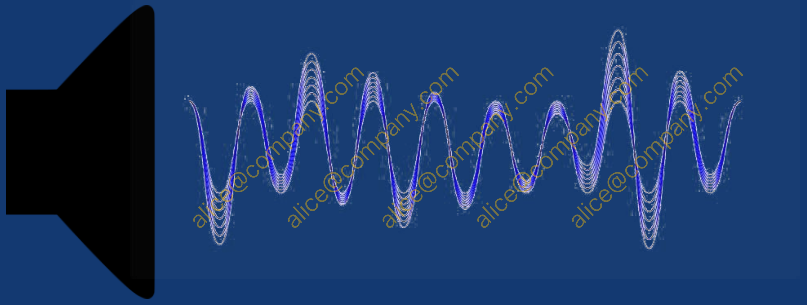
Audio Watermarking
Video Watermarking

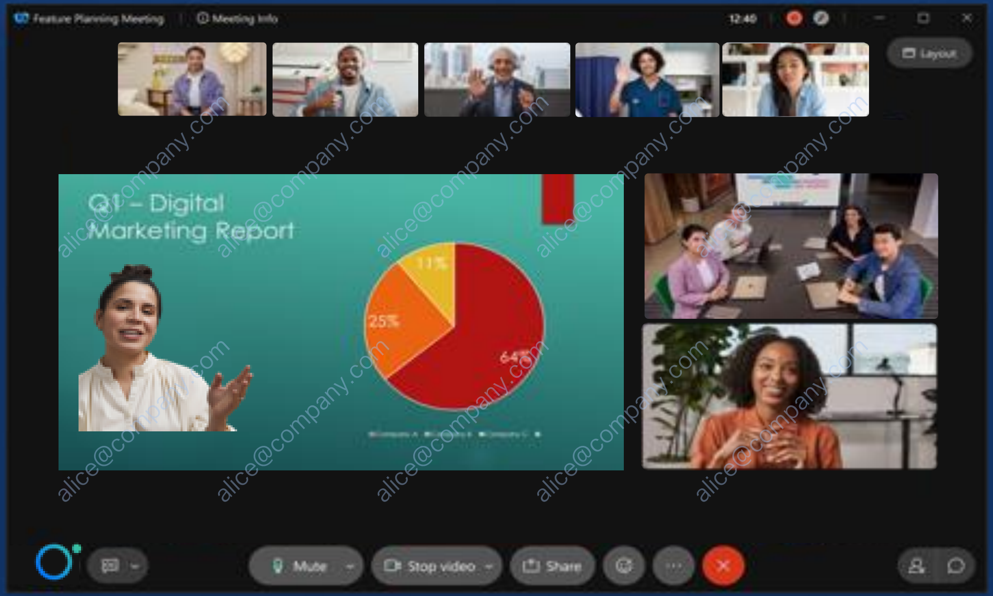
Audio & Video Water-marking

Keep your content private :

Watermarking Prevents Unwanted leakage of meeting data

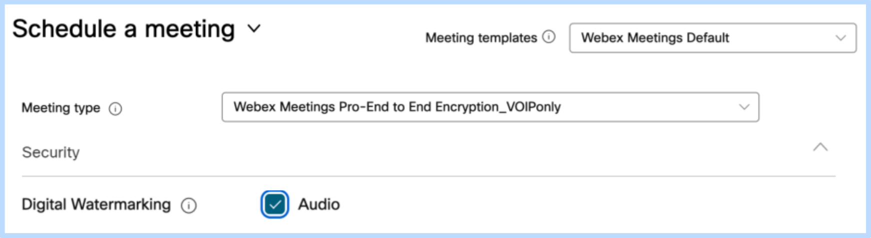
Identifies source of:
Screenshots
Video recordings
Audio recordings





Webex Meetings - Audio Watermarking

Available today for Webex E2E Encrypted Meetings



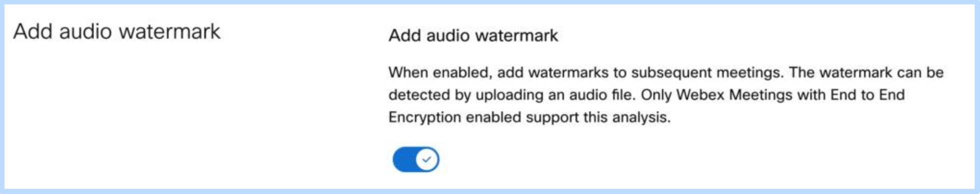
Schedule a meeting

Meeting templates: Webex Meetings Default

Meeting type: Webex Meetings Pro-End to End Encryption_VOIPonly

Security

Digital Watermarking: ☑ Audio



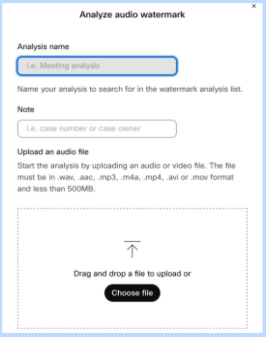
Add audio watermark

Add audio watermark

When enabled, add watermarks to subsequent meetings. The watermark can be detected by uploading an audio file. Only Webex Meetings with End to End Encryption enabled support this analysis.

When Audio Watermarking is enabled, the meeting audio includes a unique identifier for each participant.
An Admin can upload audio recordings to Control Hub, which then analyzes the recording and looks up unique identifiers.
The results of the analysis show which participant shared the meeting content externally.

- In order to be analyzed, the recording must be an AAC, MP3, M4A, WAV, MP4, AVI, or MOV file no larger than 500MB.
- The recording must be longer than 90 seconds.
- You can only analyze recordings for meetings hosted by people in your organization.
- Analyzed recordings are deleted as soon as the analysis is complete.



Analyze audio watermark

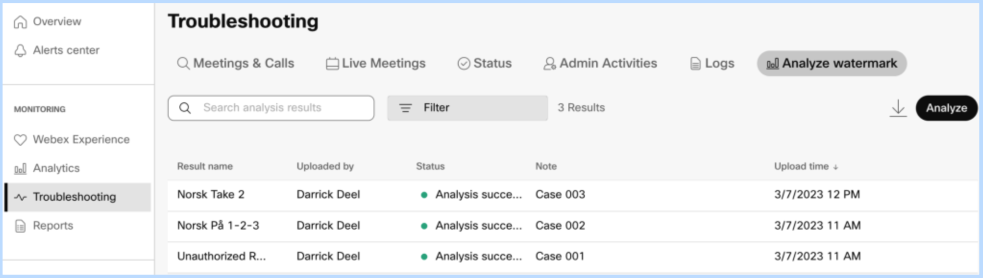
Analysis name: i.e. Meeting analysis

Name your analysis to search for in the watermark analysis list.

Note: i.e. case number or case owner

Upload an audio file

Start the analysis by uploading an audio or video file. The file must be in .wav, .aac, .mp3, .m4a, .mp4, .avi or .mov format and less than 500MB.



Troubleshooting

3 Results

Result name	Uploaded by	Status	Note	Upload time ↓
Norsk Take 2	Darrick Deel	● Analysis succe...	Case 003	3/7/2023 12 PM
Norsk På 1-2-3	Darrick Deel	● Analysis succe...	Case 002	3/7/2023 11 AM
Unauthorized R...	Darrick Deel	● Analysis succe...	Case 001	3/7/2023 11 AM

CISCO Live!

Webex Meetings - Video Watermarking

All Meeting Types supported

Visual Watermark for both shared content and video

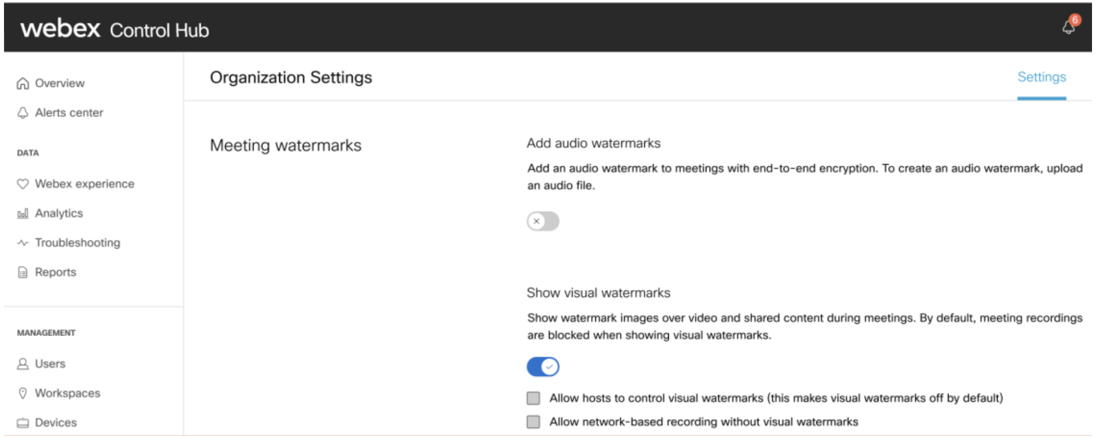
Webex app - Desktop, Mobile, Web

Authenticated users display email watermark

Unverified users display email and username

Local Recording automatically disabled

Network Recording optional



Organization Settings

Meeting watermarks

Add audio watermarks

Add an audio watermark to meetings with end-to-end encryption. To create an audio watermark, upload an audio file.

Show visual watermarks

Show watermark images over video and shared content during meetings. By default, meeting recordings are blocked when showing visual watermarks.

☐ Allow hosts to control visual watermarks (this makes visual watermarks off by default)

☐ Allow network-based recording without visual watermarks

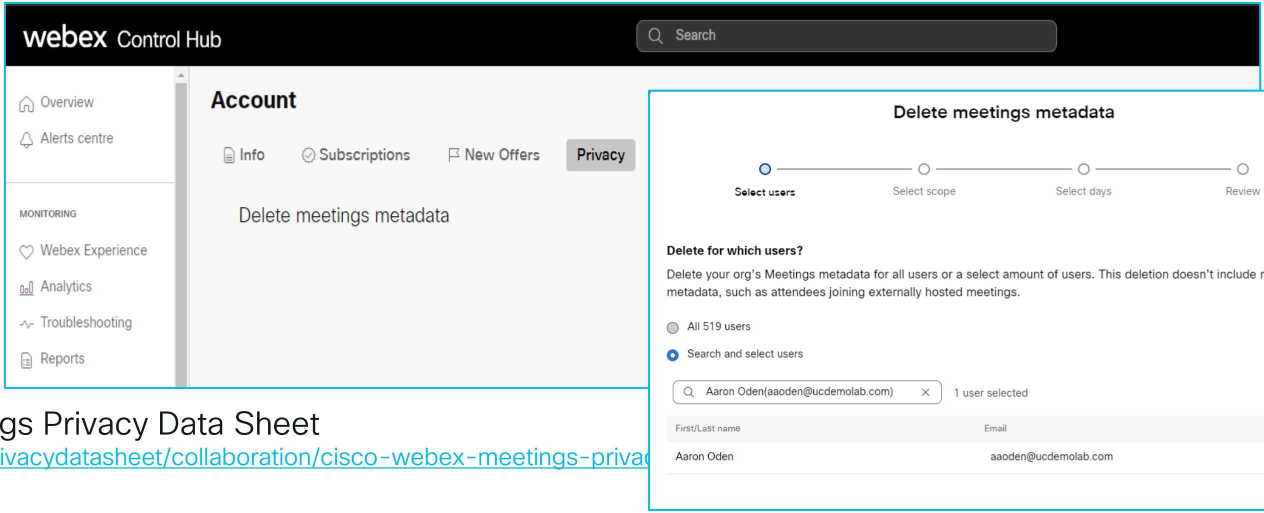
New Webex Meetings features : Privacy

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



Delete meetings metadata

Delete for which users?

Delete your org's Meetings metadata for all users or a select amount of users. This deletion doesn't include r
metadata, such as attendees joining externally hosted meetings.

○ All 519 users
● Search and select users

Aaron Oden(aaoden@ucdemolab.com) ✕ 1 user selected

First/Last name	Email
Aaron Oden	aaoden@ucdemolab.com

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

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust End to End Encryption

MLS based E2E Encrypted Meetings

- MLS key packages and User Identity Information
- MLS operation – meeting participant join
- SFrame Encryption
- Combined MLS & SFrame operation – meeting participant join

Deep Dive

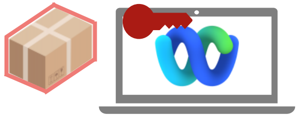
MLS key packages and User Identity Information

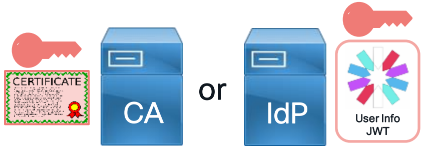
Messaging Layer Security (MLS)

Developed as a security layer for E2E encrypting group messaging.
Repurposed for Webex Meetings E2E encryption.

Identity Credentials are used by MLS (in MLS key packages) to verify meeting participants and as part of the MLS E2E encryption key generation process

RFC 9420
https://www.rfc-editor.org/rfc/rfc9420.html



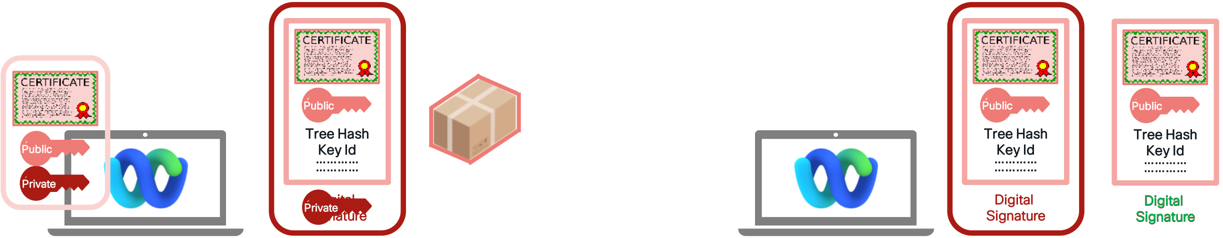


MLS uses "key packages" to identify users and to generate new meeting encryption keys as participants join and leave the meeting

Each MLS key package contains :

- Participant's Identity Info & Public Key (Verifiable Credentials/Cert.)
- A tree hash value that represents the cryptographic group state and credentials of the group members (meeting participants)
- An identifier for the current version of the meeting encryption key

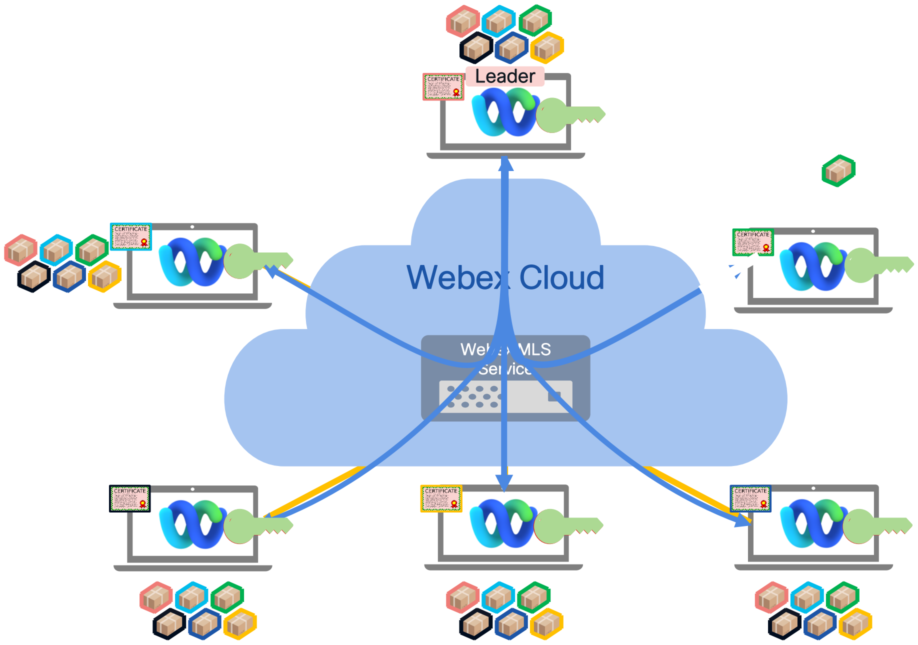
Each meeting participant signs their key package with their private key, so that other meeting participants can verify its authenticity



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

MLS Operation : Meeting Participant Join

MLS key package : contains the participant’s Identity details (verifiable credentials/ certificate) and other meta data used for identity verification and meeting encryption key generation.



New meeting participants send their key package to the meeting leader (In MLS, the leader does not need to be the Meeting Host)

The meeting leader shares the new participant’s key package with the other participants.

The meeting leader shares the existing meeting participants’ key packages with the new participant.

All meeting participants generate a new meeting encryption key
(MLS uses timers to reduce key churn when large numbers of participants join the meeting in a short time interval)

A new meeting encryption key is created when participants join or leave the meeting

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SFrame for E2E Encrypted Webex Meetings

Secure Frames
(SFrame)

Secure Media Frames provides an extra layer of authenticated encryption for media.

The whole media frame is encrypted before being placed into individual SRTP payloads

SFrame uses MLS to provide the encryption keys that each meeting participant needs

https://datatracker.ietf.org/doc/draft-ietf-sframe-enc/

Double Encryption process

1) Unencrypted media frame
2) Packetize unencrypted media frame
3) Encrypt packets using SFrame E2E Meeting Encryption key
4) Encrypted SFrame packets -> Encrypted with SRTP keys
5) Media meta data moved to SRTP header extension (authenticated)

SFrame encryption cipher AES-256-GCM

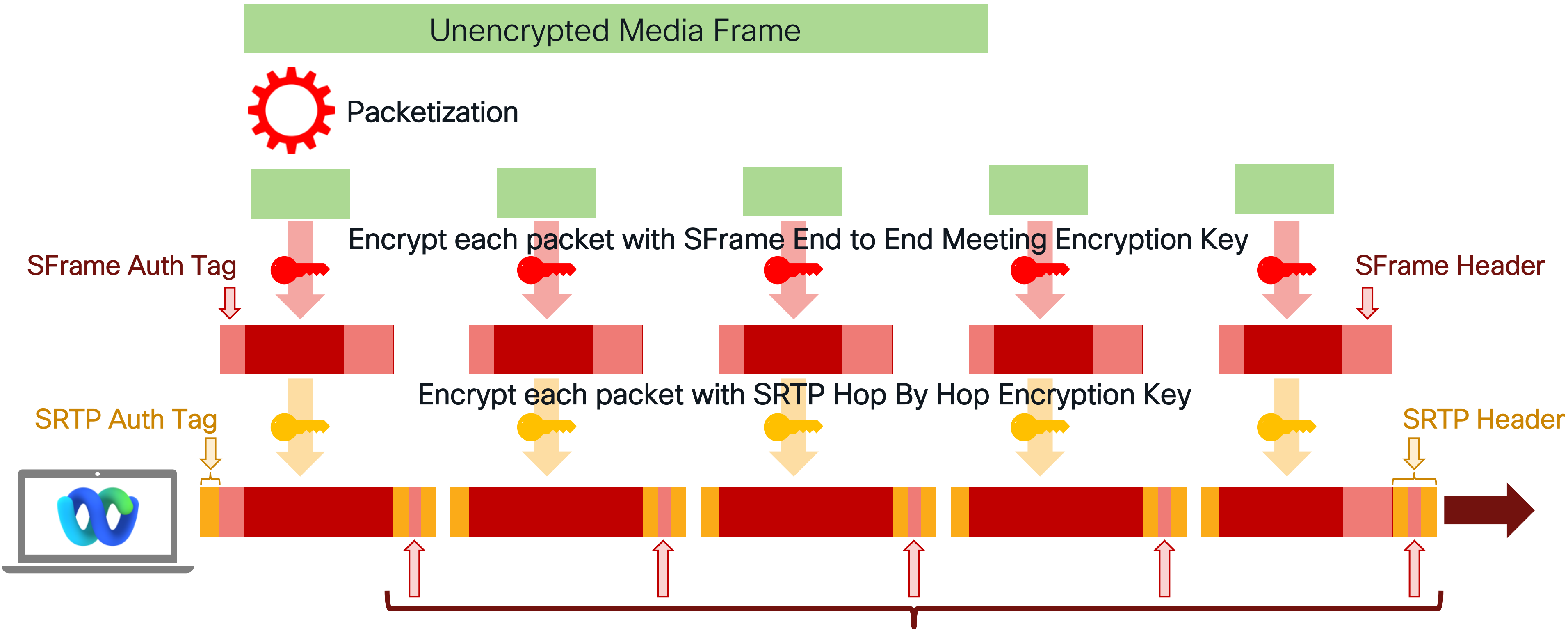
Encrypted SFrame format :

SFrame header – Frame counter (used for encryption IV) – Key Id
SFrame Encrypted Media
SFrame authentication tag

Authenticated SRTP header extension

Speaker volume indication (used by Webex media servers to switch media without decrypting SFrame content)

Secure Frames (SFrame)


Unencrypted Media Frame
Packetization
Encrypt each packet with SFrame End to End Meeting Encryption Key
SFrame Auth Tag
SFrame Header
Encrypt each packet with SRTP Hop By Hop Encryption Key
SRTP Auth Tag
SRTP Header

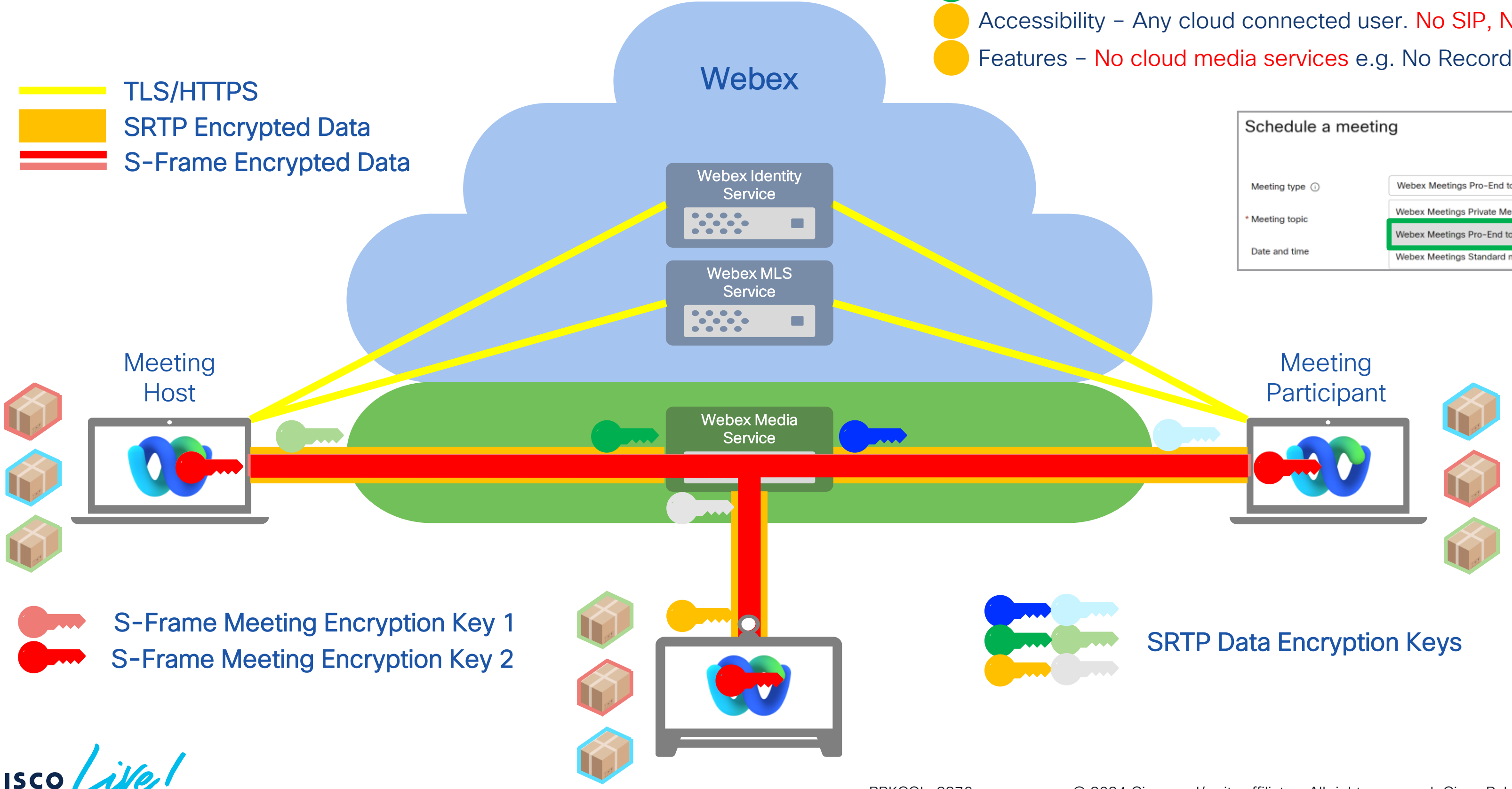
SFrame media metadata (e.g. speaker volume) in RTP Header Extension allows Webex media servers to switch data without needing to decrypt the SFrame content

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security for Webex Meetings – E2E Media Encryption

MLS and SFrame operation

- 🟢 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



TLS/HTTPS

SRTP Encrypted Data

S-Frame Encrypted Data

S-Frame Meeting Encryption Key 1

S-Frame Meeting Encryption Key 2

SRTP Data Encryption Keys

Schedule a meeting

Meeting type ⓘ — Webex Meetings Pro-End to End Encryption_VOIPonly

* Meeting topic

Date and time

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

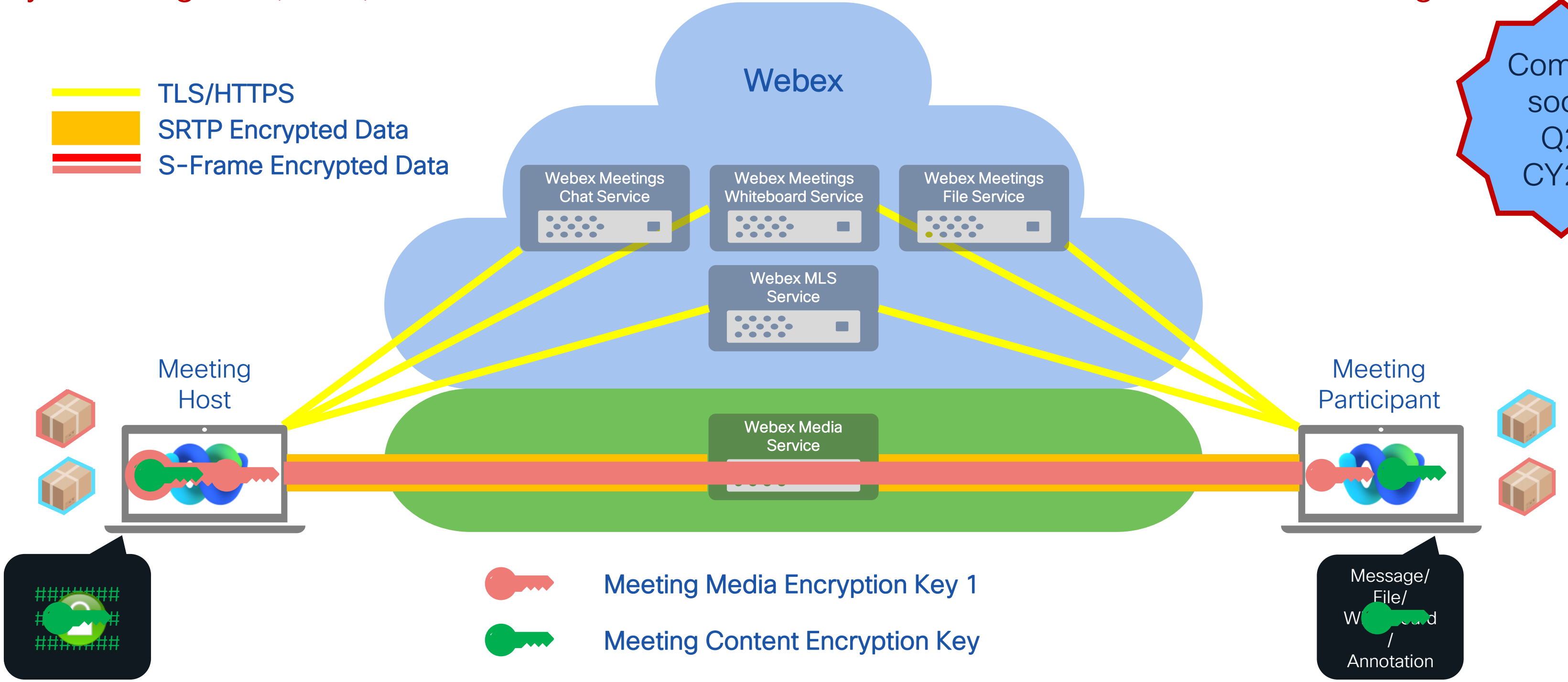
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security for Webex Meetings

E2E Encryption for meeting chat, files, whiteboards and annotation

Content encryption key generated by meeting host, encrypted with media encryption key and shared with other participants. Webex cloud services do not have access to content encryption key. Meeting chat, files, whiteboards and annotations are not available when the meeting ends

Coming soon Q2 CY24



TLS/HTTPS

SRTP Encrypted Data

S-Frame Encrypted Data

Webex

Webex Meetings Chat Service

Webex Meetings Whiteboard Service

Webex Meetings File Service

Webex MLS Service

Webex Media Service

Meeting Host

Meeting Participant

########
########
########

Message/
File/
Whiteboard
/
Annotation

Meeting Media Encryption Key 1

Meeting Content Encryption Key

Zero Trust Security for Webex Meetings
Summary of E2E Encryption features

End to End Encryption meetings available to enterprise and consumer customers
Supported by Webex App (desktop and mobile) and Webex devices
Up to 1000 participants
Audio Watermarking, Video Watermarking
Face recognition, Gesture recognition
Room interpretation, People presence detection
Proximity pairing, Background noise removal
Local Recording (Webex App)

Zero Trust E2EE does not give Webex access to meeting encryption keys. This means that cloud services and endpoints that need to decrypt meeting content cannot participate in E2EE meetings : e.g.
PSTN and SIP endpoints
Cloud Recording
Webex Assistant
Meeting Transcription, Real-time translation, Closed captioning, Highlights
Remote Desktop Control (planned)
Web Browser based Webex App
SX, DX, and MX series devices

Zero Trust Security for Webex Meetings E2E Encryption feature roadmap

<u>Medium Term</u>
E2E Encryption for 1:1 calls (Webex App and Webex devices)
E2E Encryption Breakout rooms

<u>Long Term</u>
MLS support for all meetings :
=> E2E Identity for all meetings
=> Dynamic E2E Encryption capability for all meetings

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust End to End Identity

- OpenID Connect based Credentials for User Identity Information
- Certificate (ACME) based Credentials for User Identity Information
- Webex Trust based Credentials for User Identity Information

- In Meeting Security information

Deep Dive

Zero Trust Security : E2E Identity for E2EE Webex Meetings

OpenID Connect based Credentials for User Identity Information

Coming soon Q2 CY24

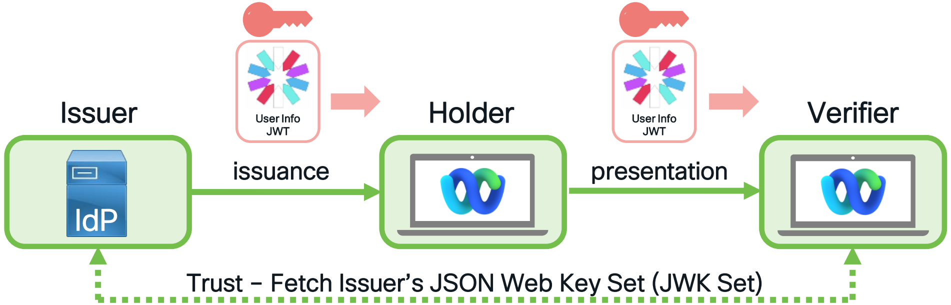
Verifiable Credentials with OpenID Connect for Webex Meetings

OpenID Connect
User Info
Verifiable Credentials

OpenID IdP based specification for the issuance and verification of User Identities based on JSON Web Tokens (JWTs)

https://openid.net/specs/openid-connect-userinfo-vc-1_0.html

https://datatracker.ietf.org/doc/draft-barnes-mls-userinfo-vc/



Identity Provider based verifiable User Identity

A verifiable credential Holder must authenticate with their IdP and request their verifiable credentials (Signed JSON Web Token).

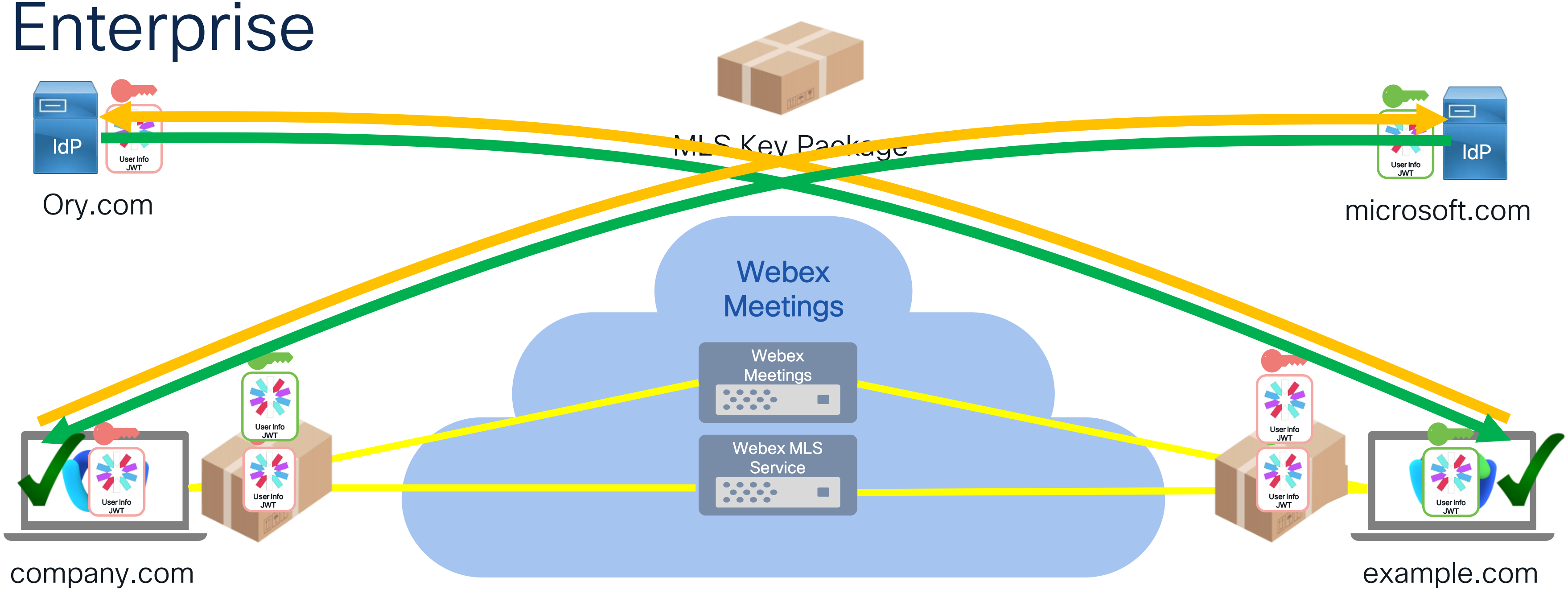
Webex uses MLS to distribute Credentials to all Meeting participants

A Verifier on receipt of another user's credentials can fetch and use the IdP's public key to verify the signature on the user's credentials

Each Webex meeting participant will verify the credentials of all other participants with their issuing IdP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex Independent identity verification – Inter Enterprise

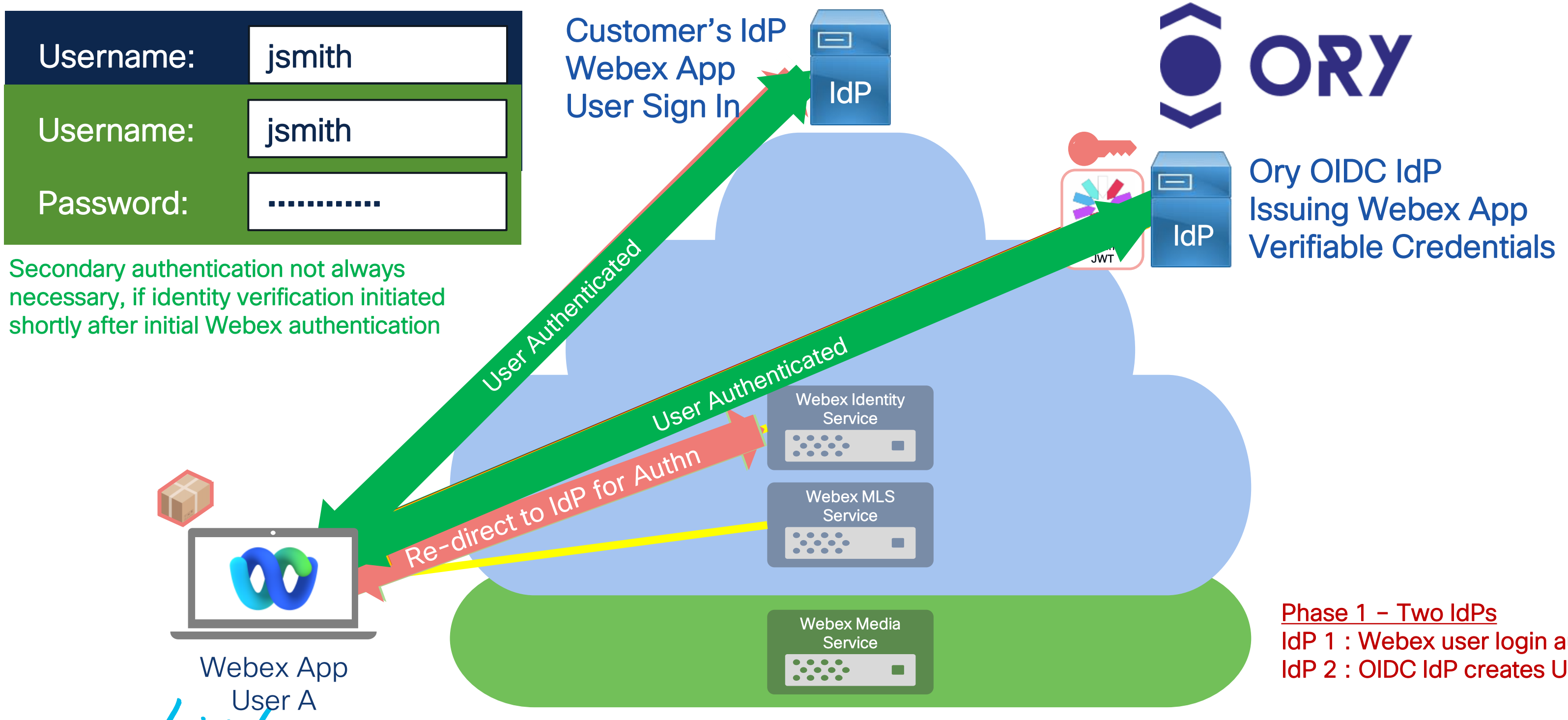


User Info Verifiable Credentials transported in MLS key packages
Credentials verified by all participants

OpenID Connect based Credentials for User Identity Information

Users authenticating with their Enterprise IdP receive :
Webex OAuth Tokens for service access

Users authenticating via their OpenID Ory IdP receive :
Verifiable Credentials for MLS identity in E2EE'ed meetings



Username:	jsmith
Username:	jsmith
Password:	•••••••••••••

Secondary authentication not always necessary, if identity verification initiated shortly after initial Webex authentication

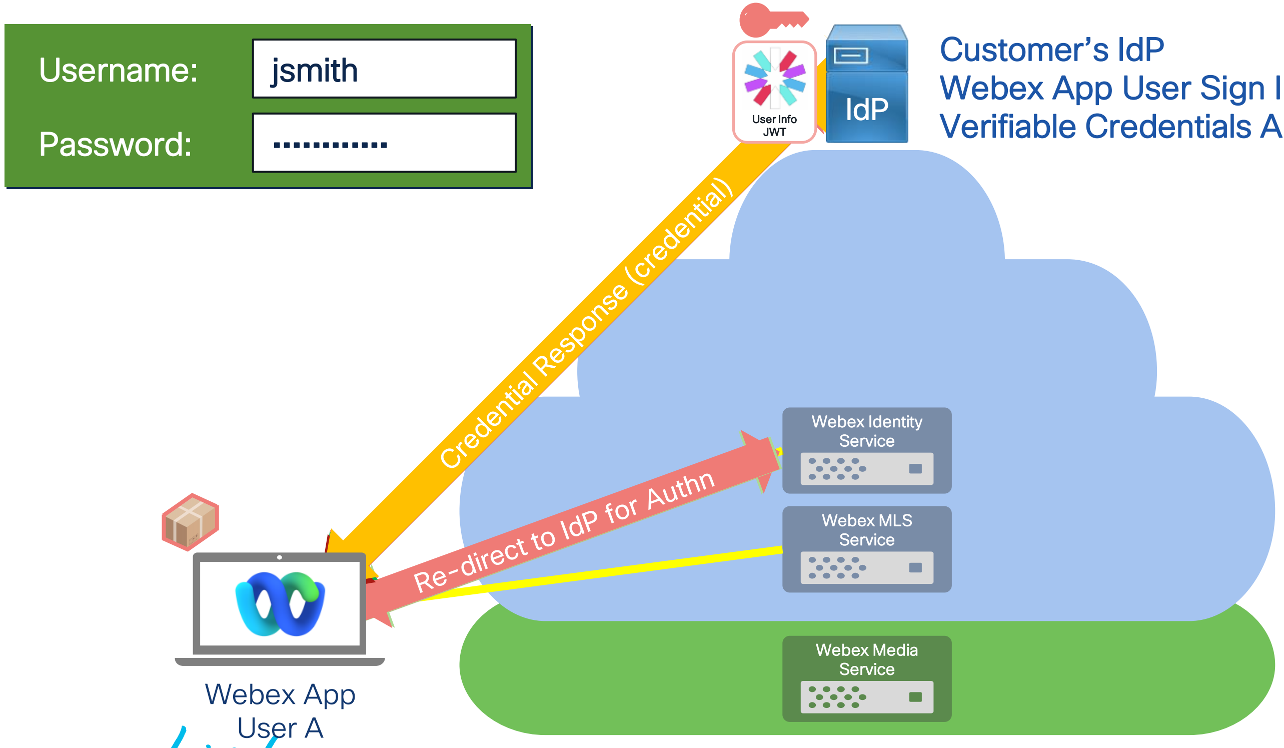
Phase 1 – Two IdPs
IdP 1 : Webex user login auth & VC login auth
IdP 2 : OIDC IdP creates User VC

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OpenID Connect based Credentials for User Identity Information

Users authenticating with their Enterprise IdP receive :
Webex OAuth Tokens for service access

and
Verifiable Credentials for MLS identity in E2EE'ed meetings



Customer's IdP
Webex App User Sign In Authentication
Verifiable Credentials Authentication

Phase 2 – Single IdP
1) Webex user login authentication
2) Verifiable Credentials login authentication

Zero Trust Security : E2E Identity for E2EE Webex Meetings

Cert (ACME) based Credentials for User Identity Information

ACME for E2E Identity for devices with Webex Meetings

Automated Certificate Management Environment (ACME)

The ACME protocol is used to generate user and device identity certificates. ACME automatically handles Certificate Signing Requests sent to Certificate Authorities

Device certificate name validation via public domain name check

User CSR validation via SAML assertion from a federated IdP

https://tools.ietf.org/html/rfc8555

https://tools.ietf.org/html/draft-biggs-acme-sso-00

ACME is protocol that can be used by a Certificate Authority and a Certificate applicant to automate the process of identity verification and certificate issuance…

RFC 8555

Describes an automated validation procedure that allows domain-name based certificates (e.g. device1.cisco.com) to be obtained without user intervention.

Webex uses MLS to distribute Certificates to all Meeting participants

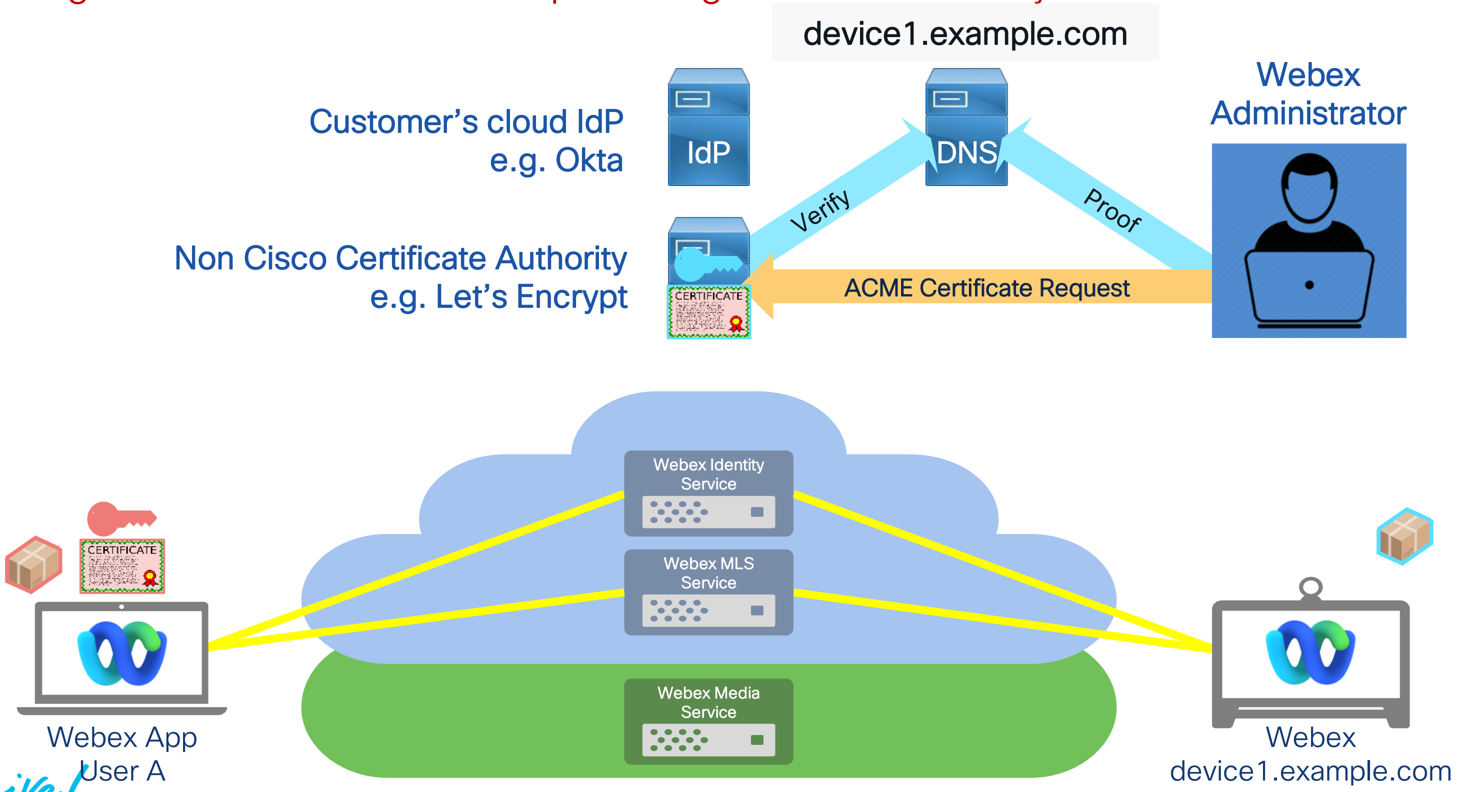
Each Webex meeting participant will verify the certificates of all other participants with their issuing CA.

Certificates validated in accordance with RFC 5280 & RFC 6960

Certificate based Credentials for Device Identity Information

Webex Devices onboarded by organization administrator receive
Webex OAuth Tokens for service access

Customer organization uses ACME to request a signed Device Identity certificate from a non Cisco CA



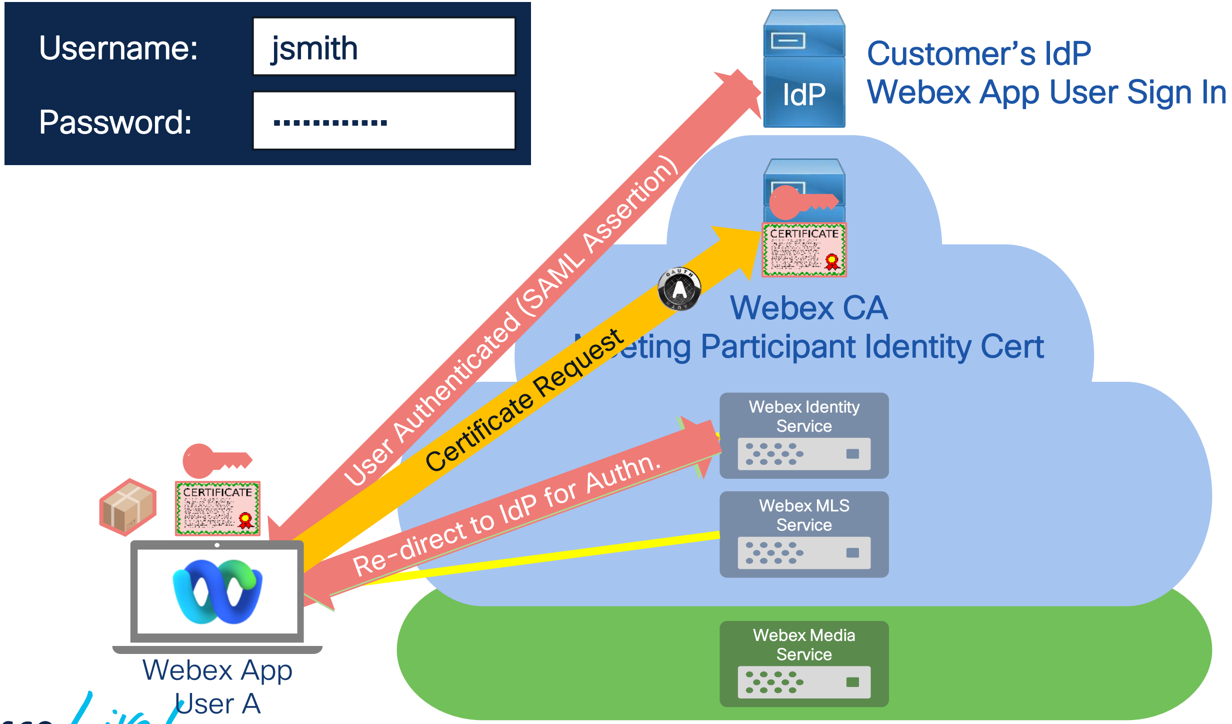
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security : E2E Identity for E2EE Webex Meetings

Webex Trust based Credentials for User Identity Information

Webex Trust based Credentials for User Identity Information

Users authenticating with their Enterprise IdP receive :
Webex OAuth Tokens for service access
and
Webex CA certificates for User Identity in Webex E2EE meetings



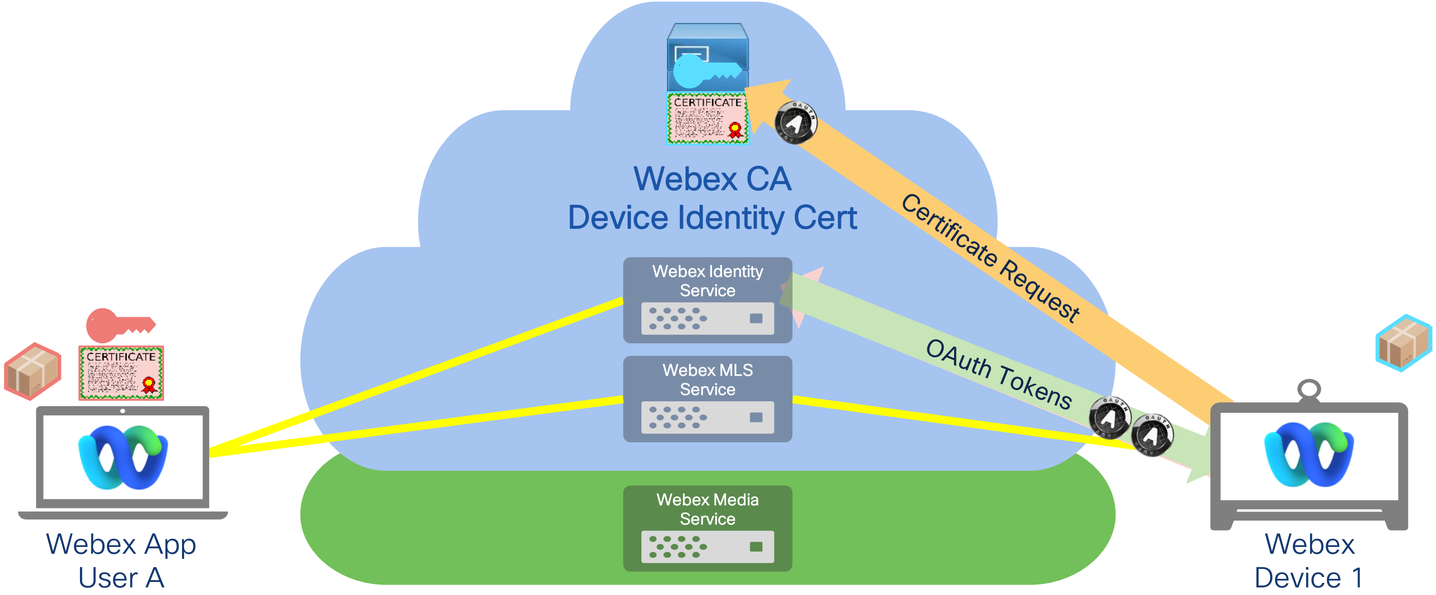
Username: jsmith

Password: ·············

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

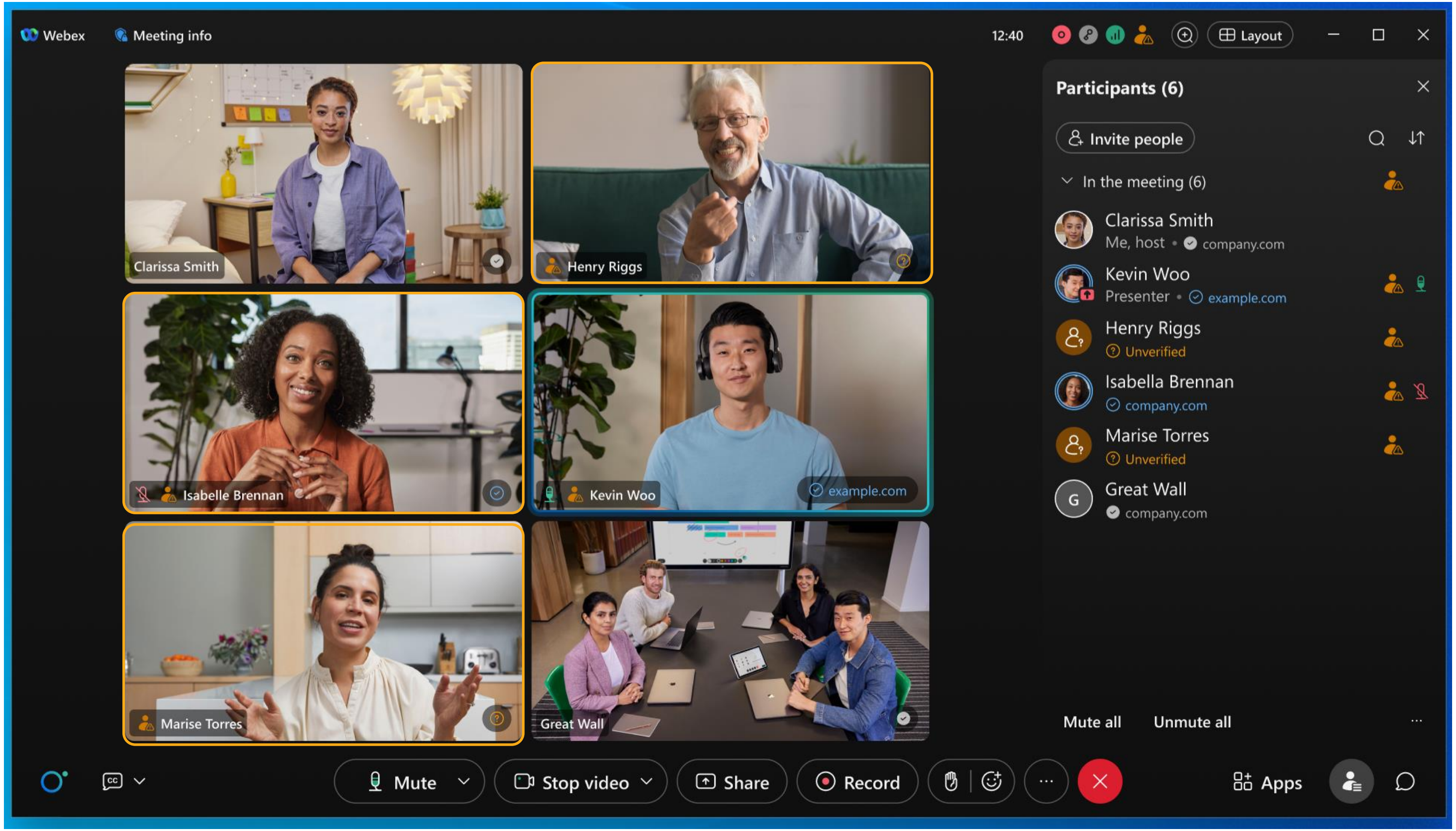
Webex Trust based Credentials for Device Identity Information

Webex Devices onboarded by organization administrator receive
Webex OAuth Tokens for service access
and
Webex CA certificates for Device Identity in Webex E2EE meetings



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security for Webex Meetings : E2E Identity Meeting Roster - User Identity details



Participants (6)

Invite people

In the meeting (6)

Clarissa Smith
Me, host • ✓ company.com

Kevin Woo
Presenter • ✓ example.com

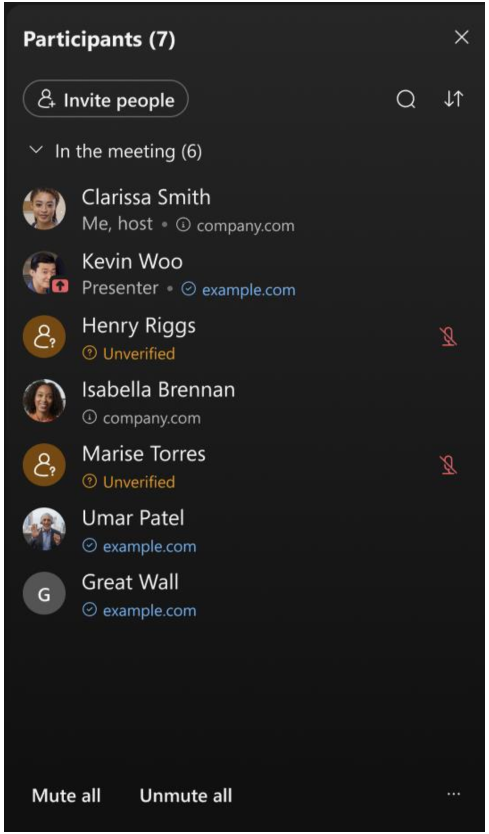
Henry Riggs
? Unverified

Isabella Brennan
✓ company.com

Marise Torres
? Unverified

Great Wall
✓ company.com

Zero Trust Security for Webex Meetings : E2E Identity Meeting Roster - User Identity details



Participants (7)

Invite people

In the meeting (6)

Clarissa Smith
Me, host • company.com

Kevin Woo
Presenter • example.com

Henry Riggs
Unverified

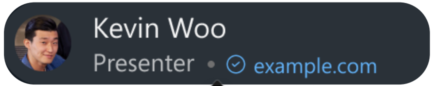
Isabella Brennan
company.com

Marise Torres
Unverified

Umar Patel
example.com

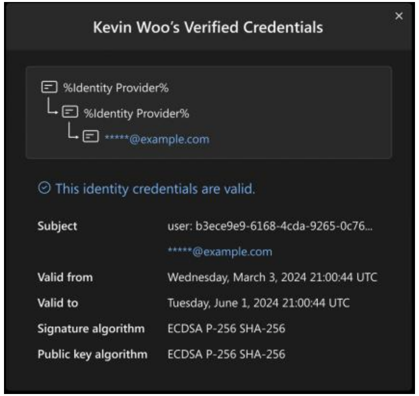
Great Wall
example.com

Mute all   Unmute all   ...



Kevin Woo
Presenter • example.com

Verifiable Credential generated by Identity Provider (Ory). Select the icon to view the credential details.

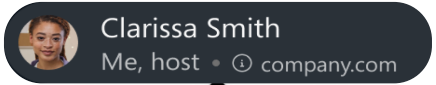


Kevin Woo's Verified Credentials

%Identity Provider%
└ %Identity Provider%
  └ *****@example.com

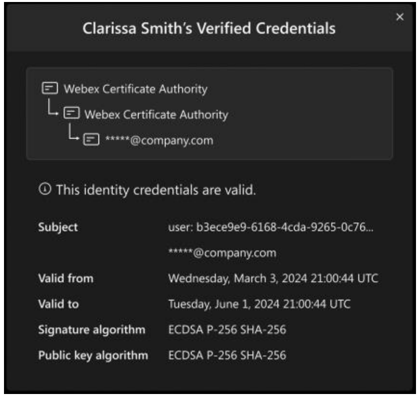
This identity credentials are valid.

Subject	user: b3ece9e9-6168-4cda-9265-0c76... *****@example.com
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256



Clarissa Smith
Me, host • company.com

Verifiable Credential generated by Webex CA. Select the icon to view the credential details.



Clarissa Smith's Verified Credentials

Webex Certificate Authority
└ Webex Certificate Authority
  └ *****@company.com

This identity credentials are valid.

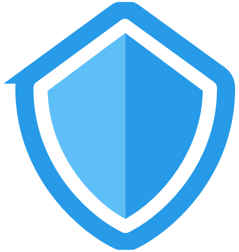
Subject	user: b3ece9e9-6168-4cda-9265-0c76... *****@company.com
Valid from	Wednesday, March 3, 2024 21:00:44 UTC
Valid to	Tuesday, June 1, 2024 21:00:44 UTC
Signature algorithm	ECDSA P-256 SHA-256
Public key algorithm	ECDSA P-256 SHA-256

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security : E2E Identity for E2EE Webex Meetings

In Meeting Security Information

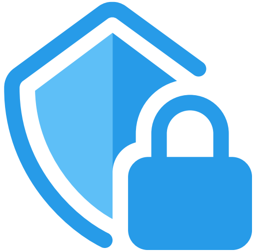
Zero Trust Security for Webex Meetings
Meeting Security icons : Encrypted/ E2E Encrypted



Encrypted Meeting :

Webex App, Webex Room devices, SIP devices, PSTN

Network based : Recording, Transcription, Speech Recognition, Closed Captions, Webex Assistant etc



End to End Encrypted Meeting :

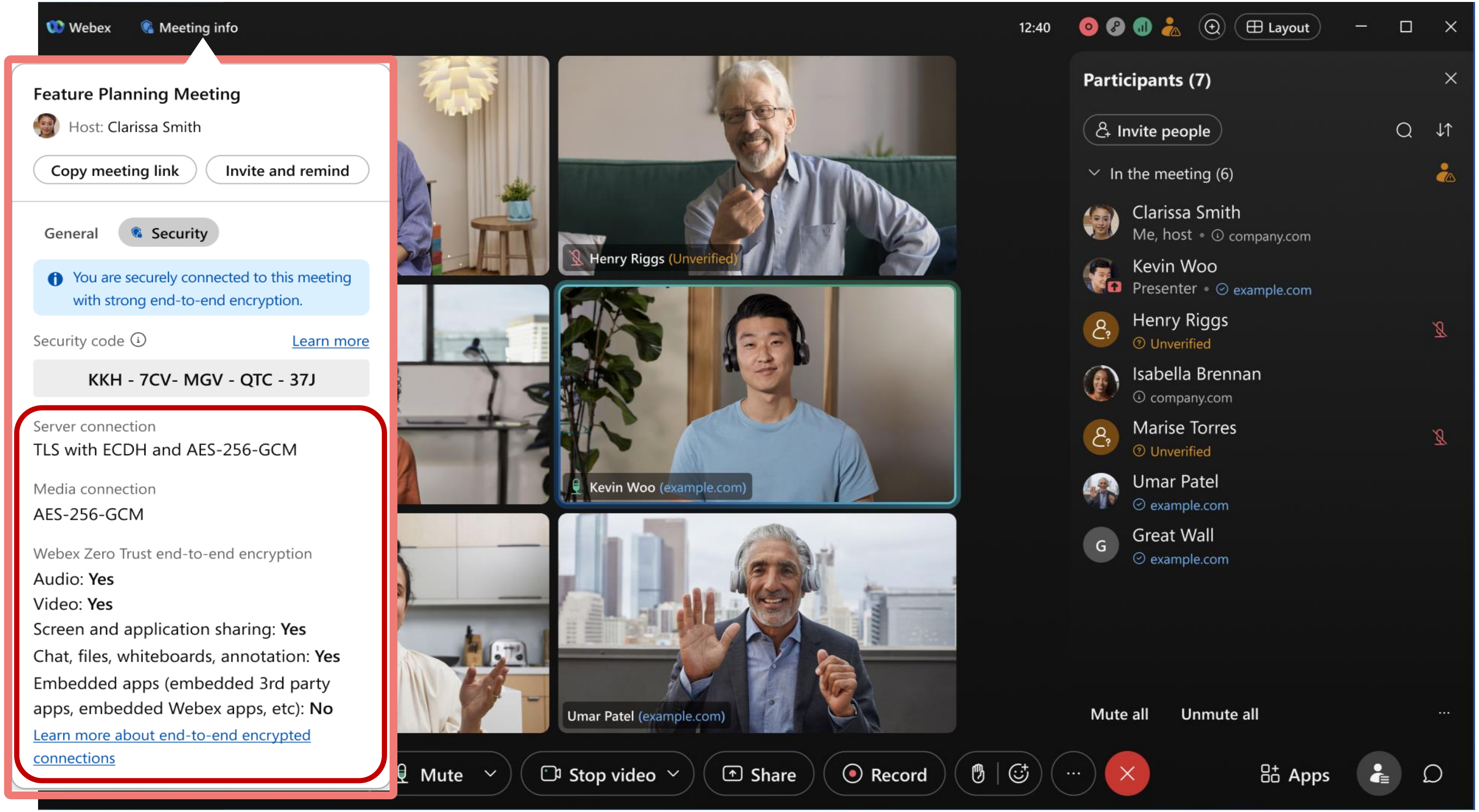
Webex App, Cloud registered Webex Room devices only

No SIP devices or PSTN users

No cloud collaboration media based services

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Security Information



Feature Planning Meeting

Host: Clarissa Smith

Copy meeting link | Invite and remind

General | Security

You are securely connected to this meeting with strong end-to-end encryption.

Security code ⓘ Learn more

KKH - 7CV- MGV - QTC - 37J

Server connection

TLS with ECDH and AES-256-GCM

Media connection

AES-256-GCM

Webex Zero Trust end-to-end encryption

Audio: **Yes**

Video: **Yes**

Screen and application sharing: **Yes**

Chat, files, whiteboards, annotation: **Yes**

Embedded apps (embedded 3rd party apps, embedded Webex apps, etc): **No**

Learn more about end-to-end encrypted connections

Participants (7)

In the meeting (6)

Clarissa Smith
Me, host • company.com

Kevin Woo
Presenter • example.com

Henry Riggs
Unverified

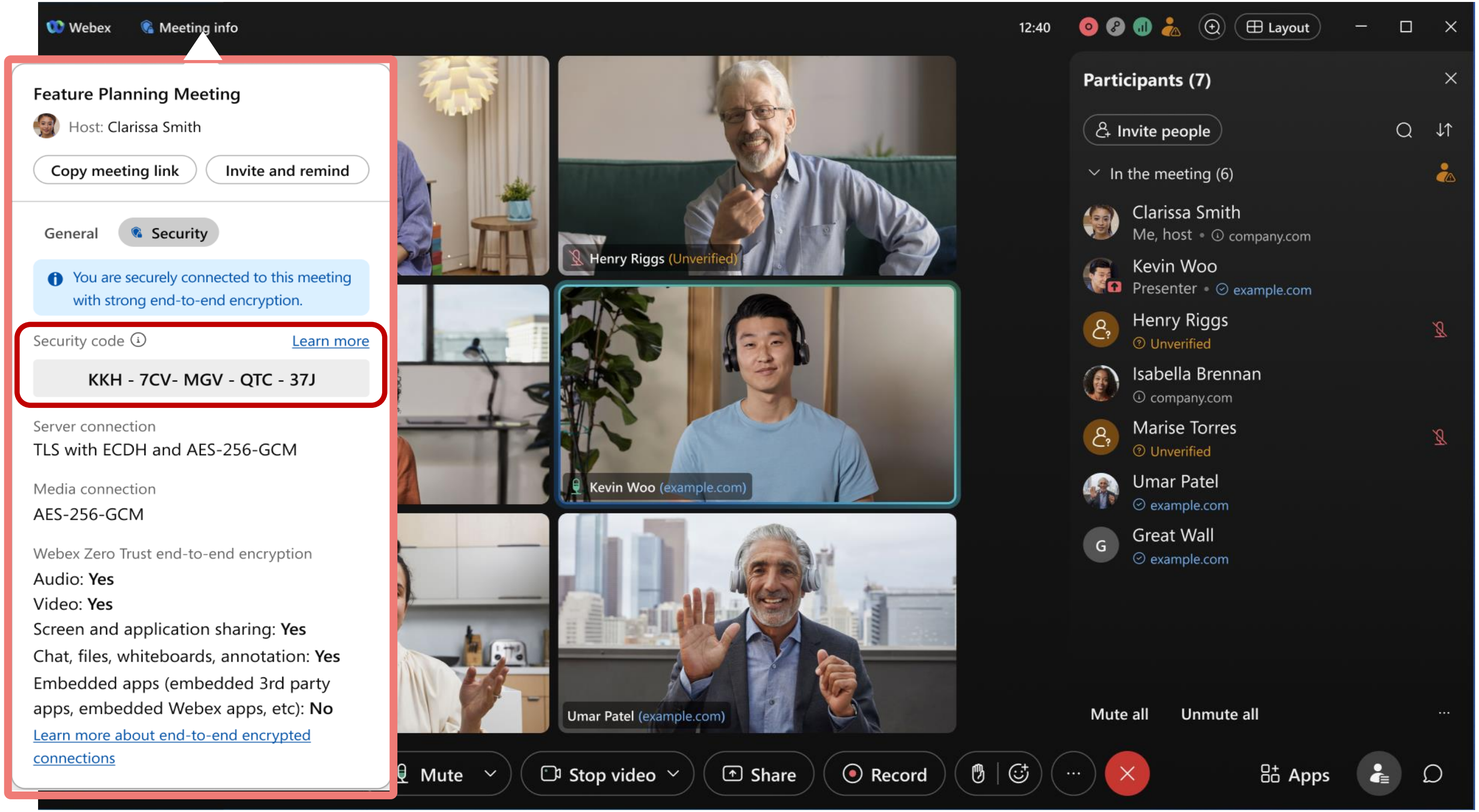
Isabella Brennan
company.com

Marise Torres
Unverified

Umar Patel
example.com

Great Wall
example.com

Zero Trust Security for Webex Meetings
E2E Encrypted Meetings - Meeting Security Code



Feature Planning Meeting

Host: Clarissa Smith

Copy meeting link | Invite and remind

General | Security

You are securely connected to this meeting with strong end-to-end encryption.

Security code ⓘ [Learn more]

KKH - 7CV- MGV - QTC - 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

Webex Zero Trust end-to-end encryption
Audio: **Yes**
Video: **Yes**
Screen and application sharing: **Yes**
Chat, files, whiteboards, annotation: **Yes**
Embedded apps (embedded 3rd party apps, embedded Webex apps, etc): **No**

Learn more about end-to-end encrypted connections

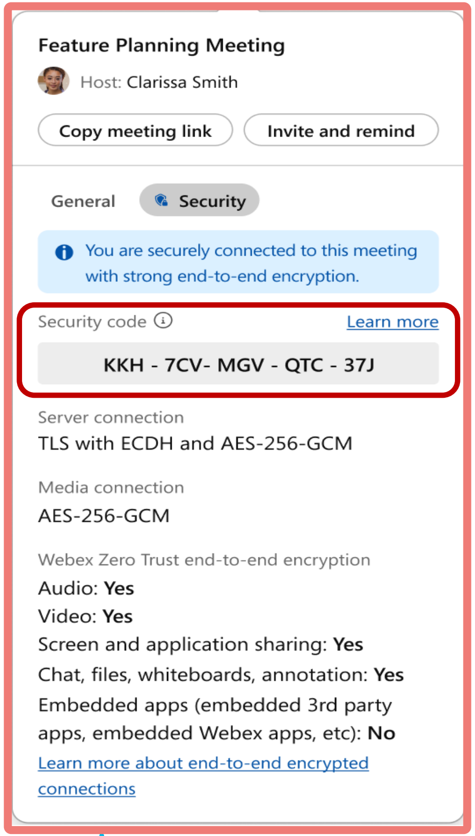
Participants (7)

In the meeting (6)

- Clarissa Smith — Me, host • company.com
- Kevin Woo — Presenter • example.com
- Henry Riggs — Unverified
- Isabella Brennan — company.com
- Marise Torres — Unverified
- Umar Patel — example.com
- Great Wall — example.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Meeting Security Codes – Protecting against MITM attacks



Feature Planning Meeting

Host: Clarissa Smith

You are securely connected to this meeting with strong end-to-end encryption.

Security code ⓘ

KKH - 7CV- MGV - QTC - 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

Webex Zero Trust end-to-end encryption
Audio: **Yes**
Video: **Yes**
Screen and application sharing: **Yes**
Chat, files, whiteboards, annotation: **Yes**
Embedded apps (embedded 3rd party apps, embedded Webex apps, etc): **No**

Learn more about end-to-end encrypted connections

The meeting security code is displayed to all meeting participants. If they all have the same value, then they know they have not been intercepted and impersonated by an attacker (Meddler In The Middle (MITM) attack)

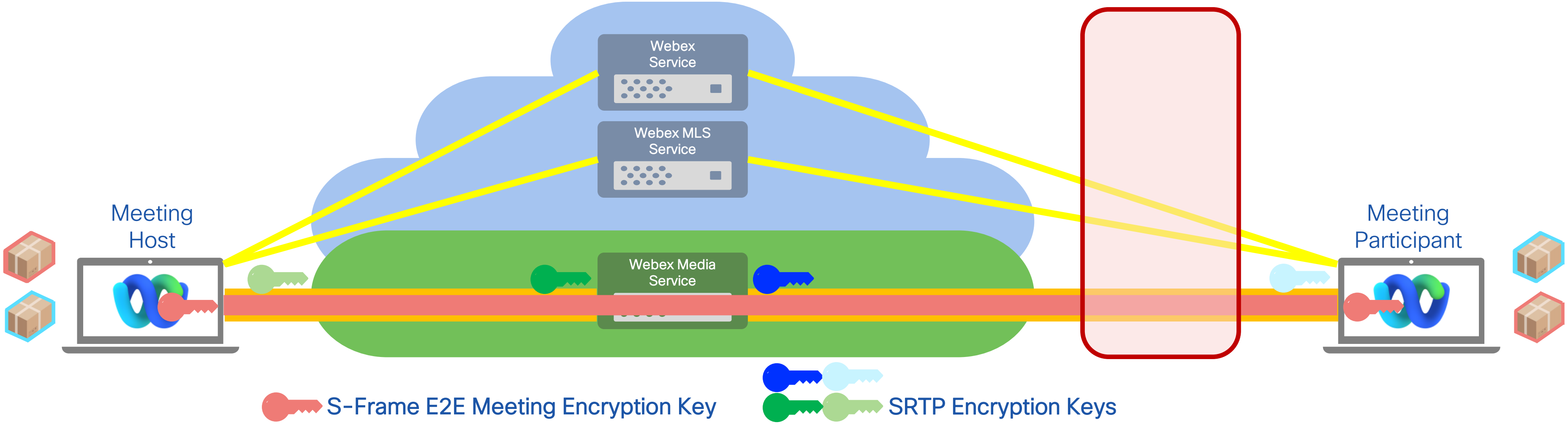
The Webex E2E Encrypted Meeting Security code is derived from all participants' MLS key packages

If participants have the same code, they know they agree on all aspects of the group, including the group's secrets and the current participant list.

The security code value changes every time a new participant joins the meeting.

Meeting Security Codes – Protecting against MITM attacks

What a MITM attacker needs to get access to :
Your encrypted media – SRTP encryption keys, all MLS E2E Meeting Encryption keys
Your TLS connections to Webex, including the MLS service and all MLS key packages



Meeting Security Codes – Protecting against MITM attacks

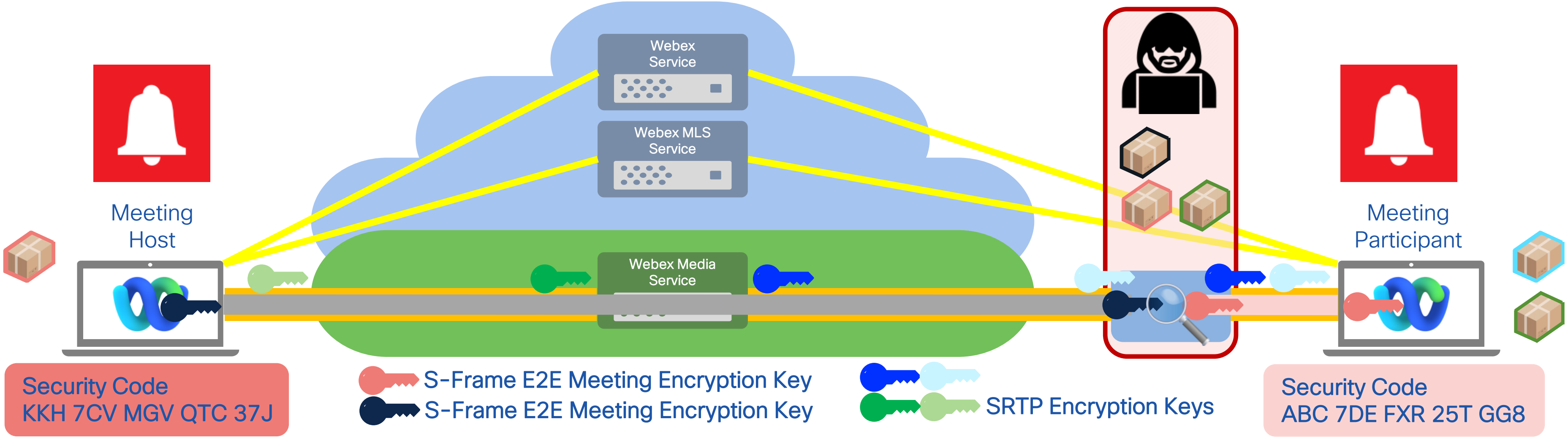
What a MITM attacker needs access to :

Your encrypted media – SRTP encryption keys, all MLS E2E Meeting Encryption keys

Your TLS connections to Webex, including the MLS service and all MLS key packages

To impersonate you – At a minimum, a MITM attacker needs to :

Intercept all MLS key packages and replace them with their own



Security Code
KKH 7CV MGV QTC 37J

S-Frame E2E Meeting Encryption Key

S-Frame E2E Meeting Encryption Key

SRTP Encryption Keys

Security Code
ABC 7DE FXR 25T GG8

The Security Codes generated by each Webex app using their MLS key packages should match

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

cisco Live!

Let’s go