

Webex Security, Identity, and Digital Resilience:

Strengthening Collaboration in a Hybrid World

Nick Halbert-Lillyman
Solutions Engineer - Collaboration

cisco Live !

Cisco Webex App

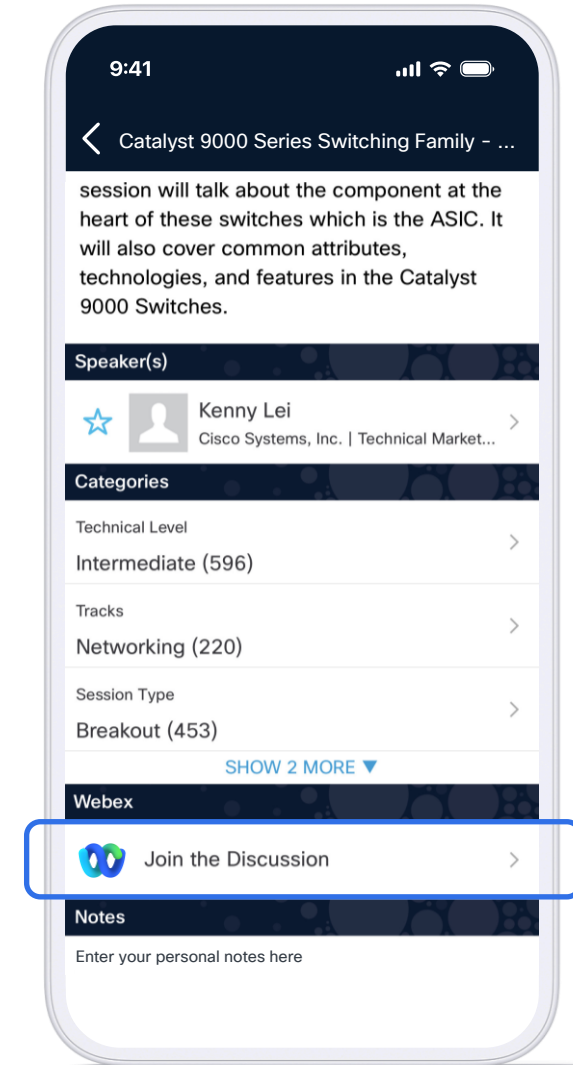
Questions?

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 by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2561>

Agenda

- 01 Introduction**
- 02 Webex Identity Integration and Role Based Access**
- 03 Webex Meetings Security and Zero Trust**
- 04 Digital Resilience for Collaboration**
- 05 Webex Australian Data Residency and Compliance**

Introduction

Collaboration in a Hybrid World

Most organizations have moved or are moving to cloud-first technology deployments – including for collaboration

This can improve capabilities, reduces costs and is perfectly suitable for business-as-usual

High service-uptime can be expected – e.g. Webex Calling/CC 99.999% SLA



Security and Trust

Most major cloud collaboration platforms provide a solid security baseline by default;

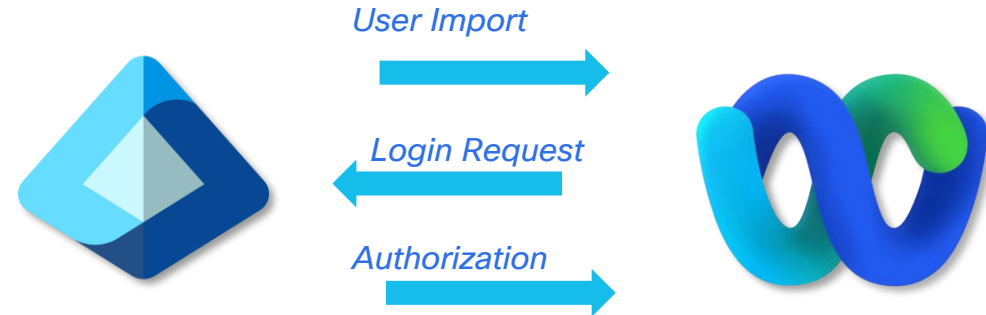
- Strong encryption for calls, meetings, messages, file sharing
- Administrative controls, MFA, SSO
- Meeting participant and lobby controls
- Security assessments and certifications – SOC 2/3 (global), IRAP (Australia) etc



Integration with Identity Providers

Typically, organizations leverage centralized identity platforms for most or all corporate services – Entra ID, Active Directory, Okta, etc

- Performs user synchronization and Single-Sign-On between your IDP and your collaboration platform
- Easy to setup and use when you have a 1:1 relationship between IDP and collab platform



**For many organizations, the
“default” is enough.**

But.....

When Collaboration is Mission-Critical....

Collaboration can be mission-critical – e.g. emergency services, hospitals, operational areas

WAN communications may not always be reliable –e.g. deployed/remote locations

High SLA's won't help if your ISP has issues, or somebody forgets to “dial before they dig” outside your building

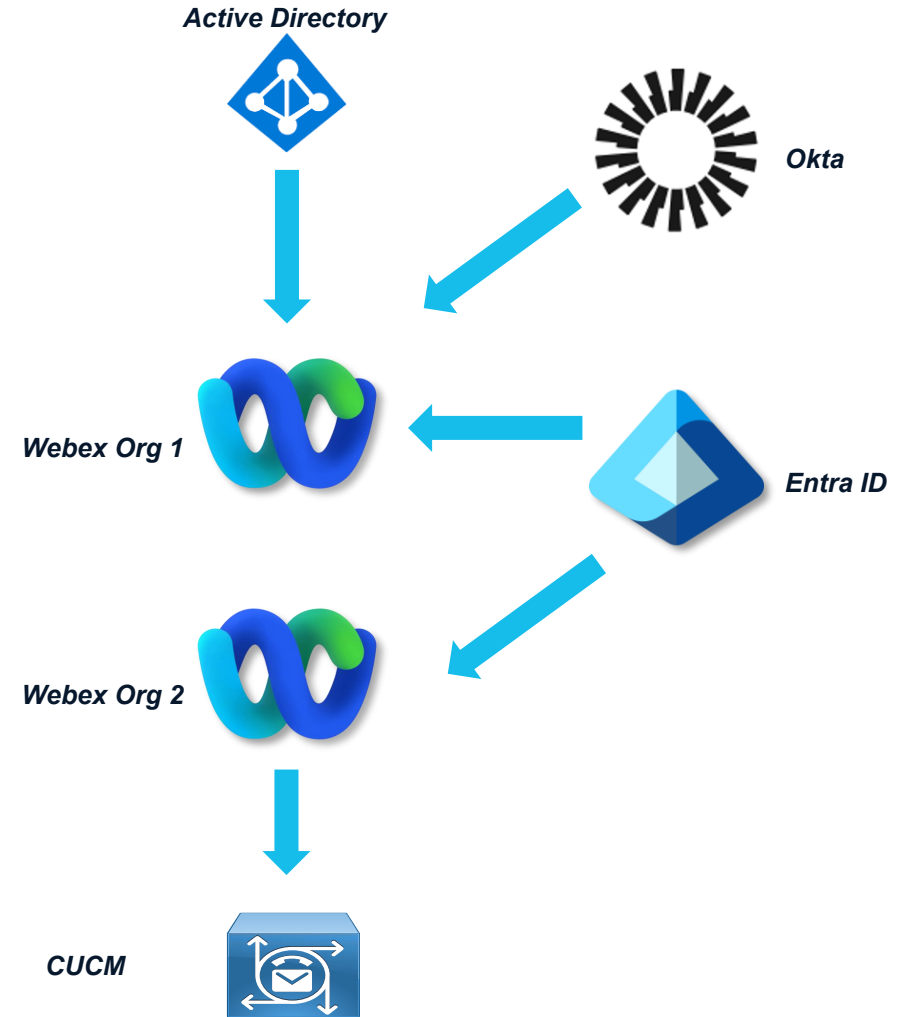
Customers can choose to keep services on-premises, but these deployments may not provide the feature set or integration with the wider enterprise that users have come to rely on



Or Your Identity and Access Requirements are Complex...

Identity Integration and Administrative Access requirements may be complex, e.g:

- Multiple IDP vendors or tenancies into a single collaboration platform
- Mix of IDP-synched and locally created users, SSO and non-SSO
- Mergers/Acquisitions, organisational change can break 1:1 relationships with IDP and collaboration platform
- Multiple partners managing different sections of your deployment
- Delegated admin access to certain locations or functions



If You Need a Higher Level of Trust...

Trust in companies, governments and institutions is dropping – many organizations want to take security in their own hands

External and Internal threats, leaks, deepfakes and identity fraud are on the rise

How do we verify not only our own users, but external people we are meeting with?

Conflicting priorities between security and empowering your workforce with modern capabilities



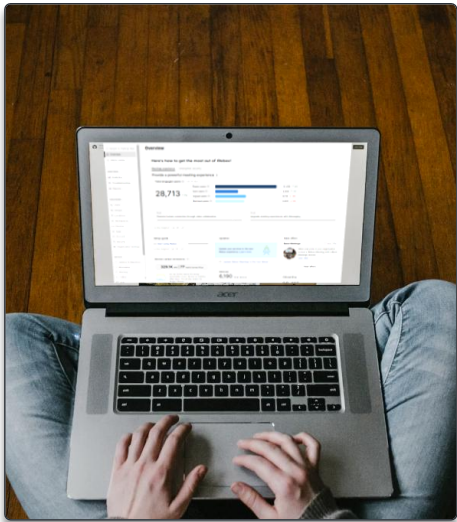
Equip the Platform to Meet Your Needs



Webex Identity Integration and Role Based Access

Integrating Webex with Identity Providers

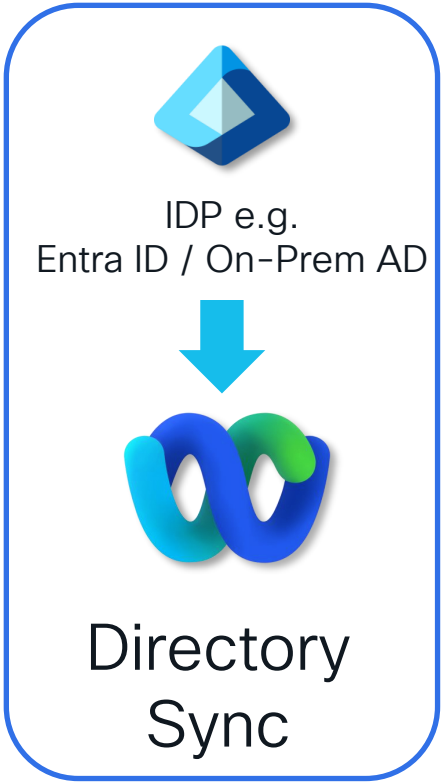
Webex Provisioning Methods



Manual



CSV



Directory Sync

Most Common Method



API:
People API/
SCIM

Entra ID (Azure AD) Wizard for Users + Groups

webex Control Hub

Search

Overview
Alerts center

MONITORING

Analytics
Troubleshooting
Reports

MANAGEMENT

Users
Groups
Locations
Workspaces
Devices
Apps
Account
Organization Settings

SERVICES

Updates & Migrations
Justin CiscoLive Lab

Organization Settings

Settings Templates Beta

Directory Synchronization

New users will be automatically added from your directory when it synchronizes. Updates can be made directly in Cisco Directory Connector.

[Download Directory Synchronization](#)
[How to Turn On Directory Synchronization](#)
[Troubleshoot Cisco Directory Connector](#)

Directory Synchronization

- Disabled

User Security ⓘ

When enabled, users who change their passwords will have to sign in to Webex again after the new passwords are detected by Directory Connector.

☒ Force authentication when users change passwords

Microsoft Azure AD integration

Integrate Azure AD to provision users and groups. Azure synchronizes periodically. [More on Azure AD setup](#)

Set up

Manage inactive user

Delete inactive user

After a user is deactivated manually or through directory synchronization, the user will be deleted from Control Hub after 30 days by default. This feature only works when directory synchronization is turned off.

Delete inactive user after

Microsoft

admin@moderncomms090877.onmicrosoft.com

Permissions requested

Review for your organization

Cisco Webex Identity Integration

This app would like to:

- ✓ Sign in and read user profile
- ✓ Read all groups
- ✓ Read all company places
- ✓ Read all users' full profiles
- ✓ Read all audit log data
- ✓ Manage apps that this app creates or owns
- ✓ Read all group memberships
- ✓ Read domains

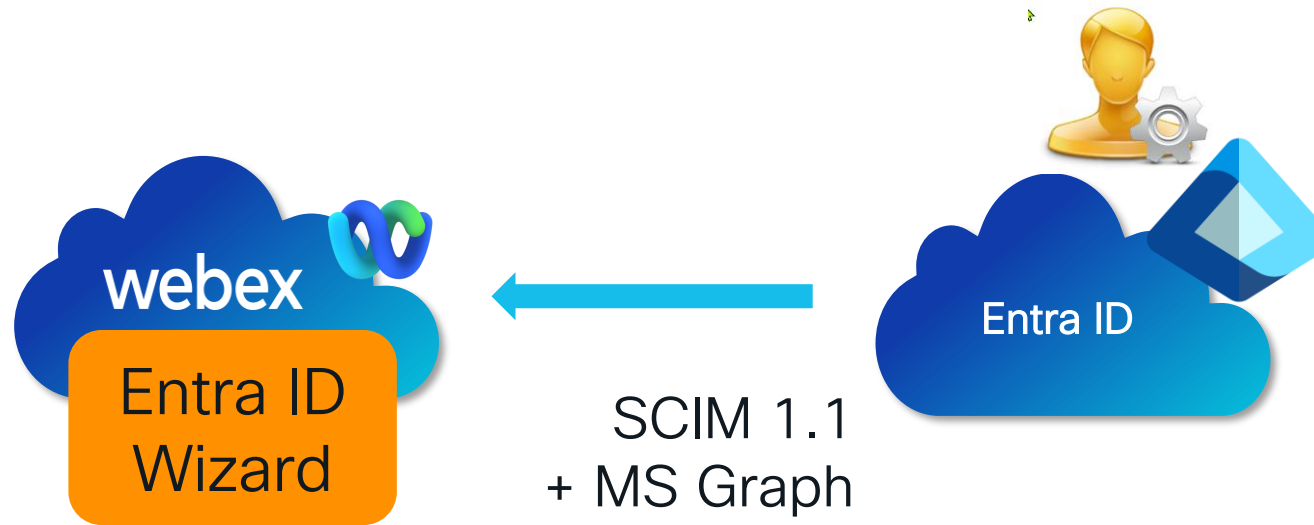
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

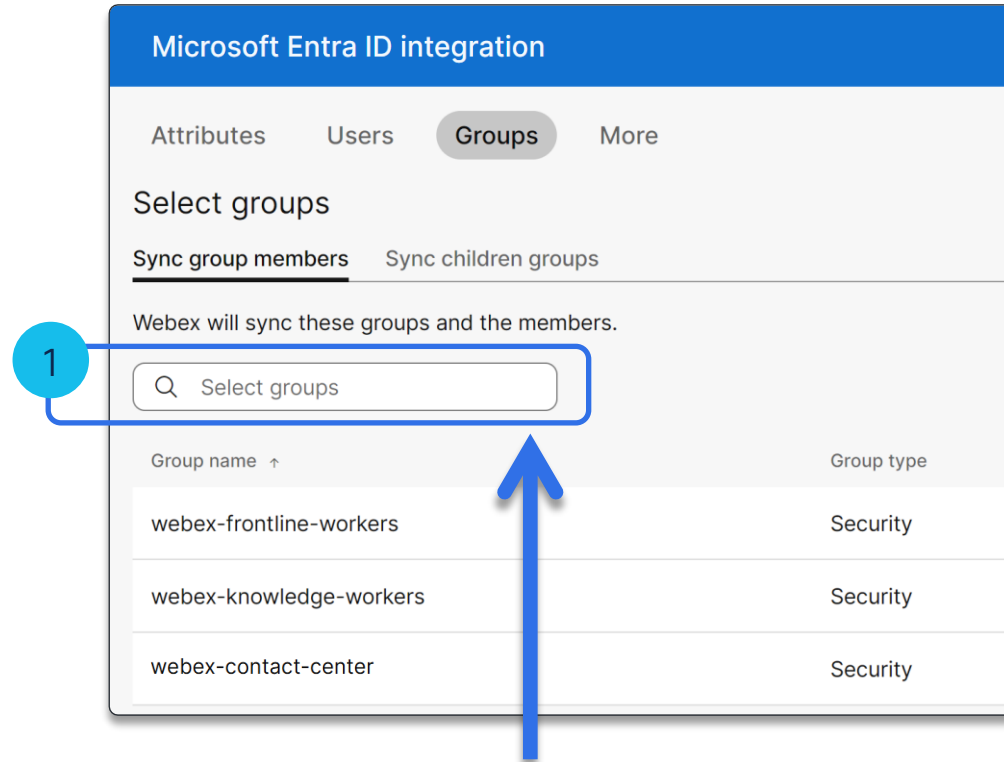
Identity Sync using Entra ID Wizard



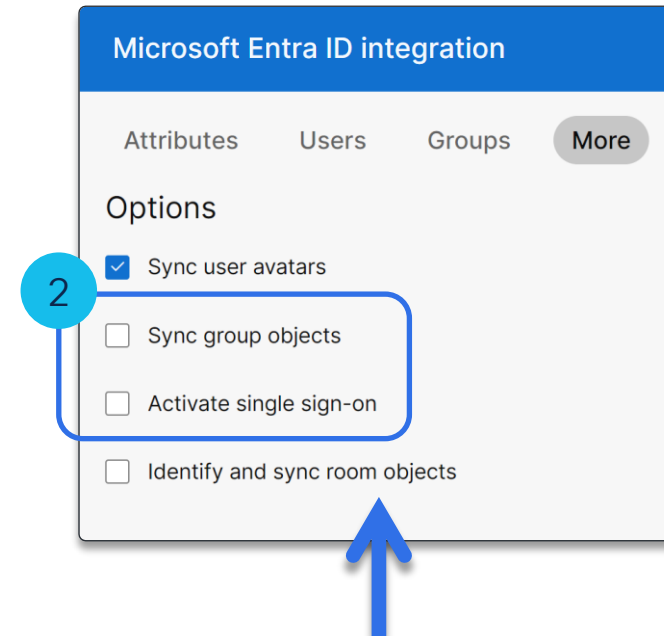
The initial Microsoft Entra ID sync is **triggered immediately** after you enable provisioning – you will be prompted to perform a “dry run” first.

Subsequent syncs are **triggered every 20-40 minutes**, depending on the number of users and groups in the application.

Enable SSO and Import Entra ID Groups



Search for the groups which you wish to Sync to Webex



Import Groups and Activate SSO via single click!

Note: If SSO already enabled via SAML, disable first

Groups - Example



Frontline
Workers

1000 Members



Basic Messaging
Free Meetings
Free 1:1 Calling in Webex



Knowledge
Workers

500 Members



Messaging
Meetings
Webex Calling



Customer
Experience

100 Members



Messaging
Meetings
Webex Calling
+ **Contact Center Premium**

Applying License Templates to your Group

1

webex Control Hub

Overview

Alerts center

MONITORING

Analytics

Troubleshooting

Reports

MANAGEMENT

Users

Groups

Locations

Workspaces

2

Groups

Webex groups

Synchronized groups

Search by name

5 groups

Name ↑	Source ⓘ
webex-contact-center	Entra ID
webex-frontline-workers	Entra ID
webex-knowledge-workers	Entra ID
webex-super-users	Entra ID
Webex-Users	Entra ID

Groups

webex-contact-center

3 members

Overview

Members

3

Assignments

Licenses

Based on your settings, applied to future and/or existing users.

How does this work? ⓘ

This group doesn't have a license yet.

Set up

Settings templates

Applied to existing and future members

How does this work? ⓘ

Type	Template
General	None
Messaging	None
Meeting	None
Calling	None
Vidcast	None

License Assignment

Modify licenses assignment

Group licenses assignment

Select the licenses you want to assign to your users.

Messaging

2

Meeting

5

Calling

2

Customer Experience

1

^

Subscription: Call on Webex (1:1 call, non-PSTN)

☒

Call on Webex (1:1 call, non-PSTN)

^

Subscription: Register to Unified Communications Manager (UCM)

☐

Register to Unified Communication Manager (UCM)

^

Subscription: Enterprise Trial - 09/17/2024

☒

Webex Calling ⓘ

☒

Professional

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKCOL-2561

SCIM 2.0 Directory Sync

- Webex supports the SCIM 2.0 standard for user synchronization, which includes the ability to sync user groups
- Okta has pre-built SCIM 2.0 integration – search for *Cisco Webex Identity SCIM 2.0* on Okta
- Can manually build SCIM 2.0 integration from Entra ID
- SCIM operations performed entirely from client/Identity provider side via API – **no configuration on Control Hub**
- Can co-exist with other identity integrations from other domains/IDPs, e.g. Entra ID Wizard/App



SCIM Endpoints and HTTP Methods

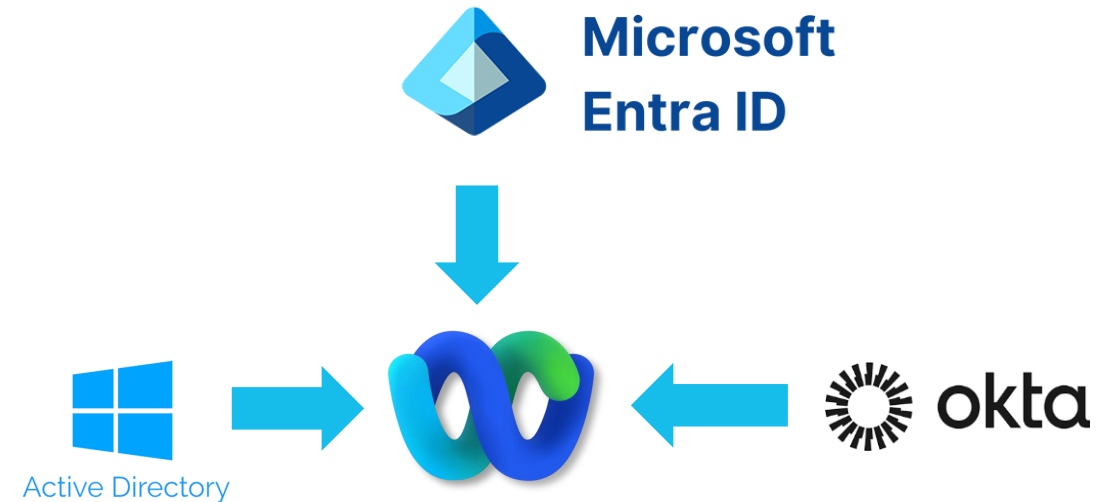
The SCIM protocol defines HTTP methods and endpoints for managing resources, such as "User" and "Group" resources that correspond to "/Users" and "/Groups".

HTTP method	SCIM Usage
GET	Retrieves one or more complete or partial resources.
POST	Depending on the endpoint, creates new resources, or may be used to bulk-modify resources.
PUT	Modifies a resource by replacing existing attributes with a specified set of replacement attributes (replace). PUT should not be used to create new resources.
PATCH	Modifies a resource with a set of client-specified changes. (partial update).
DELETE	Deletes a resource.

Webex Control Hub with Multiple Identity Sources

Entra ID Wizard Considerations

- The Entra ID Wizard is feature-rich and user friendly
- Key limitation of 1:1 Entra ID Wizard integration per Control Hub
- Webex supports Identity sync from multiple other sources;
 - Entra ID Enterprise Application
 - On-Prem AD (Directory Connector)
 - SCIM (including Okta, Entra ID)
 - Webex can sync to *or* from CUCM using Cloud Connected UC



Entra ID – Webex Provisioning Method Comparison

- The **Entra ID wizard is more capable and recommended** for your first/largest MS tenancy syncing into Control Hub
- Add additional Entra ID tenancies from that tenancy's MS Admin (Webex Enterprise App or SCIM 2.0)
- Ensure users in domain/s synced by Entra ID Wizard are not also added from other sources

Feature	Wizard	Enterprise App	SCIM 2.0
Avatar Sync	Yes	No	No
Group Sync	Yes	No – will use default group/license template in Control Hub	Yes
Domain sync + SSO	Auto	Manual	Manual
Allow multiple Entra ID tenancies to sync with single Control Hub	No	Yes	Yes
Enforced 1:1 Sync between Entra ID and Control Hub for synced domains	Yes	No	No
Configured From	Control Hub	MS Admin	MS Admin
Setup Difficulty	Low	Moderate	High

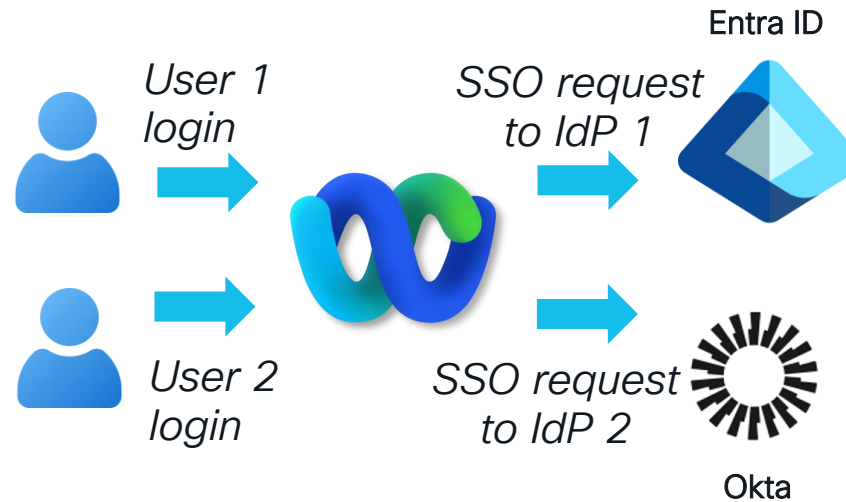
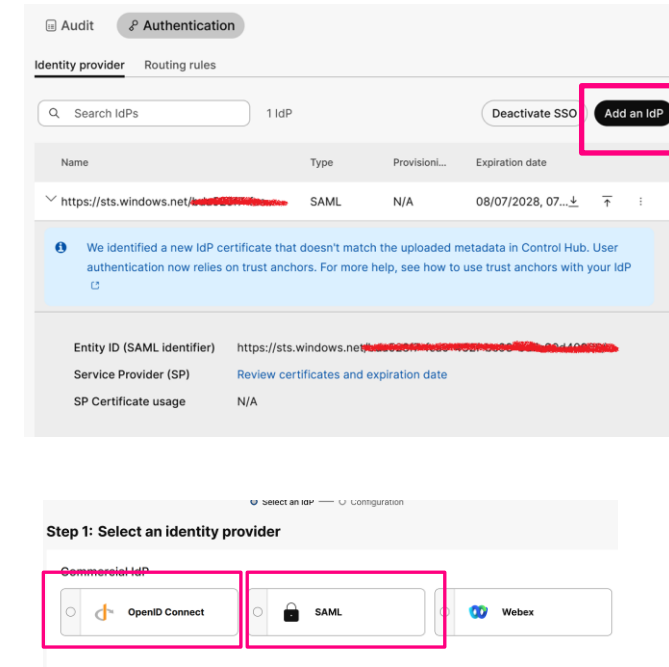
Single Sign On with Multiple IdPs

- Webex supports SSO with your SAML IdP
- By default, SSO is implanted org-wide
- SSO with multiple IDPs now supported – SAML and/or OIDC
- Setup org-wide SSO first, then add subsequent IDP/s
- Designate SSO IDP based on a user's **group** or **domain**

Org-wide – SSO with Single IDP (default)



Per group/Domain SSO with Multiple IDP



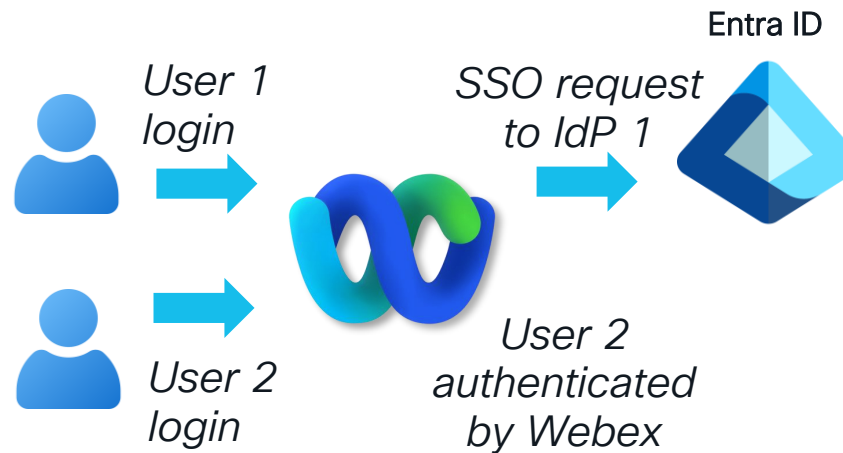
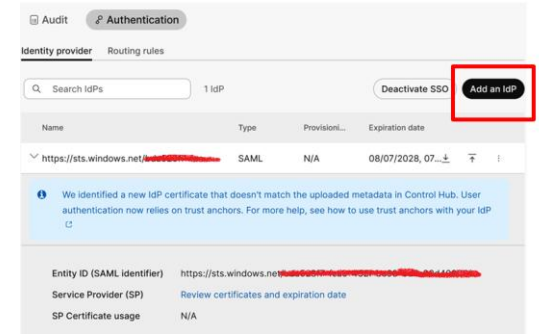
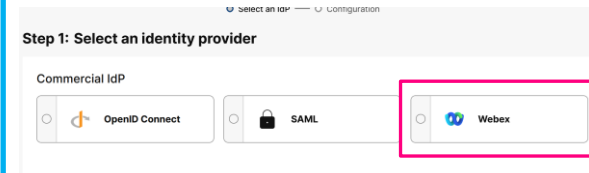
Webex as an IDP

- By default, if no SSO is configured, users leverage Webex for authentication with username/password (and optional MFA)
- **Webex IDP also available with “Multiple IDP”** feature – choose “Webex” when adding secondary IDP
- Allows for mix/match between SSO/non-SSO users. Per domain/group as per other secondary IDPs
- Mix of synched and locally created users
- Ideal for testing, generic accounts, temporary/external users

Org-wide – SSO with Single IDP (default)



Per group/Domain SSO with Multiple IDP



Role Bases Access Enhancements

Webex Role Based Access

- Cisco is currently delivering a flexible, customer-defined RBAC solution to address current and future customer and partner administrative access requirements.
- Cisco's RBAC solution offers a custom role builder based on assigned permissions and a delegated administration solution to segment access to an organization's assets.



Custom Role-Based Access

Objectives:

- Maintain the **existing set of Webex Static Roles**
- **Respect principle of least privilege** allowing fine-grained control permissions
- Provide avenues to **assign roles to groups of users**
- **Conditional rendering** of control hub limited to the controls the admin has permission to use
- Customers have the ability to **create and define their own custom roles**

The screenshot shows the 'Create admin role' dialog with the 'Permissions' tab selected. It is at 'Step 2: Add permissions'. A note states: 'Select permissions directly from the list below or quickly filter it by keywords. Note that within a permission group, the edit permission has a dependency on the view permission, while the delete permission (if applicable) has a dependency on both view and edit permissions.' There are two columns: 'Available Permissions (74)' and 'Added Permissions (7)'. The 'Available' column lists categories like Organization Management, Alerts, Analytics, and Hybrid Services with their respective permissions. The 'Added' column shows selected permissions: View alerts, View users, Create and edit users, View Meetings Analytics, View Calling Analytics, View Hybrid Services, and Edit Hybrid Services. 'Previous' and 'Create' buttons are at the bottom right.

The screenshot shows the 'Assign admin roles' dialog. It has tabs for 'Filter by' (Custom, Organizational, Functional, Services). The 'Organizational' tab is active, showing 'Full admin' and 'Read-only admin' options. The 'Functional' tab shows various roles like Support admin, User and device admin, Device admin, Compliance officer, Security activity admin, Advanced troubleshooting, and Webex Calling detailed call. The 'Services' tab shows a table for assigning roles to specific sites. A tooltip for 'Device admin' states: 'For visibility into both Control Hub and Contact Center admin activities via Control Hub's Security section'. 'Cancel' and 'Save' buttons are at the bottom right.

Custom RBAC – Current Status

Location Admin – Available NOW

- Restrict admin activities to one or more locations

Permission Groups – In Beta NOW

- User Management
- Device Management – Workspace Insights
- Calling
- PSTN
- Analytics
- Troubleshooting
- Reporting
- License Management
- Messaging

Permission Groups Coming Soon to Beta

- Meetings
- Audit Services
- Devices
- Contact Service
- Hybrid Calendar

<https://gobeta.webex.com>

Admin Activities Role

Enables administrators to assign the Admin Activities role to users, granting them permission to view administrator activity logs

Ideal for security team, auditors

Assign admin roles

Assign admin roles to Paulo Jorge Correia

Filter by: Custom Organizational Functional Services

Custom roles

- ☐ Calling user custom role

Organizational

- ☒ Full admin ⓘ
- ☐ Read-only admin ⓘ

Functional

- ☒ Support admin ⓘ
- ☒ User and device admin ⓘ
- ☒ Device admin ⓘ
- ☐ Compliance officer ⓘ
- ☐ Security activity admin ⓘ
- ☐ Advanced troubleshooting ⓘ
- ☐ Webex Calling detailed call

For visibility into both Control Hub and Contact Center admin activities via Control Hub's Security section

Services

- ☒ Webex site admin roles ⓘ Manage scope ^

Assign Meeting content admin for all eligible sites

Webex site	Basic Webex site admin roles ⓘ	Basic Webex site admin roles ⓘ
licensegroupstestsite1.dmz.webex.com	Webex site admin	• Not assigned
licensegroupstestsite2.dmz.webex.com	Webex site admin	• Not assigned
licensegroupstestsite2.dmz.webex.com	Webex site admin	• Not assigned

Cancel Save

Role Assignment for a Group of Users

Assign roles to a group of users in Control Hub, granting all group members the administrative privileges associated with the assigned role.

Combine with group sync from Entra ID Wizard/SCIM 2.0 to use your IDP to grant administrative privileges – previously only available manually via Control Hub

Assign admin roles

Assign admin roles to Admin team

Filter by: Custom Organizational Functional Services

Custom roles

☐ Calling user custom role

Organizational

☒ Full admin ⓘ
☐ Read-only admin ⓘ

Functional

☒ Support admin ⓘ
☒ User and device admin ⓘ
☒ Device admin ⓘ
☐ Compliance officer ⓘ
☐ Security activity admin ⓘ
☐ Advanced troubleshooting ⓘ
☐ Webex Calling detailed call

For visibility into both Control Hub and Contact Center admin activities via Control Hub's **Security** section

Services

☒ Webex site admin roles ⓘ Manage scope ^

Assign Meeting content admin for all eligible sites

Webex site	Basic Webex site admin roles ⓘ	Basic Webex site admin roles
licensegroupstestsite1.dmz.webex.com	Webex site admin	• Not assigned
licensegroupstestsite2.dmz.webex.com	Webex site admin	• Not assigned
licensegroupstestsite2.dmz.webex.com	Webex site admin	• Not assigned

Webex Meetings Security and Zero Trust

Webex Meetings User Access Restrictions

Feature Controls for Internal Webex Meetings

The screenshot displays the Webex Control Hub interface. On the left, a sidebar lists services: Updates & Migrations, Messaging, Meeting (selected), Calling, Connected UC, and Hybrid. The main content area is titled 'Meeting: Disable Recording' with a subtitle 'No Recording : Int & Ext - Rank 3'. It features a 'Settings' tab and an 'Applied groups' section. The settings are organized into several categories: Collaboration tools (Annotation, Polling, Q&A), In meeting (Chat, Closed captioning, File transfer, Participant list, Take presenter, Highlights and voice commands), Recording (Cloud recording, Local recording), Remote control (Enable remote control, Application remote control, Desktop remote control, Web browser remote control), Enable sharing (Application sharing, Desktop sharing, File sharing, Web browser sharing, Camera, Whiteboard sharing), and Settings override (Override participant settings when hosting). All features are currently enabled, indicated by blue toggle switches and checkmarks.

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

Feature Controls for External Webex Meetings

The screenshot displays the Webex Control Hub interface. On the left, a sidebar lists services: Updates & Migrations, Messaging, Meeting (selected), 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'. The settings are organized into four sections: Collaboration tools, Remote control, In meeting, and Video. Each section contains a list of features with toggle switches and checkboxes, all of which are currently enabled. The 'In meeting' section includes a link to 'Apply this setting to guest users'.

webex Control Hub

SERVICES

- Updates & Migrations
- Messaging
- Meeting**
- Calling
- Connected UC
- Hybrid

Meeting

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

Remote control

- ☒ Enable remote control
Host and participant
 - ☒ Application remote control
 - ☒ Desktop remote control
 - ☒ Web browser remote control

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

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

Also available to users with free “Basic” or “Attendee” license

Webex Meetings: Security, Encryption and User Verification Basics

Encryption for standard Webex Meetings

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

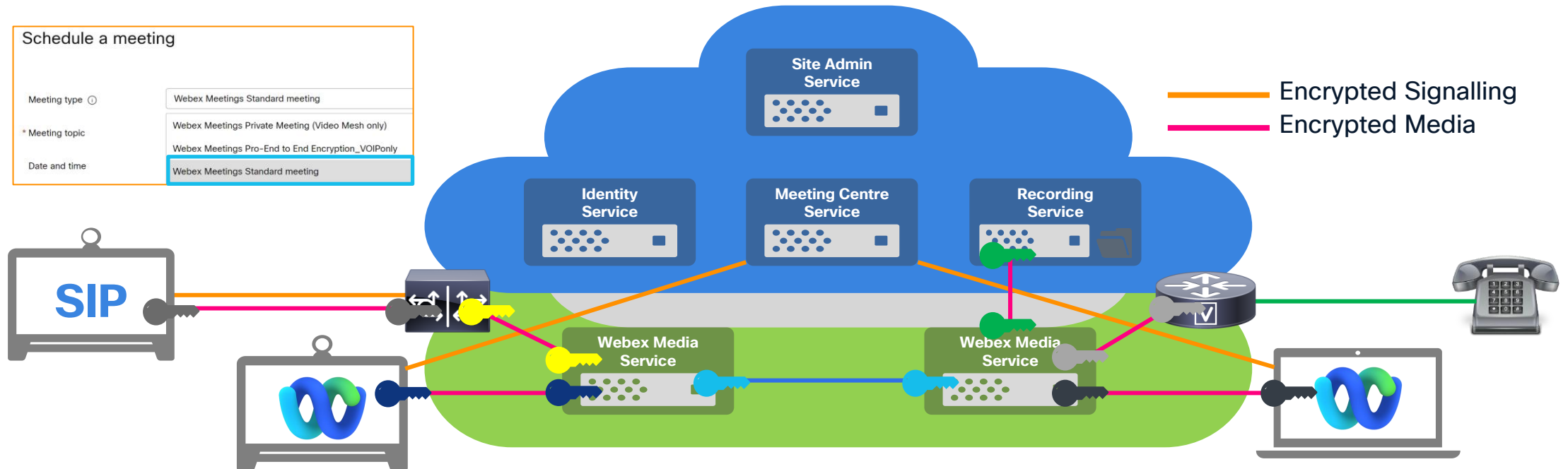
Webex apps and devices use encrypted signalling and encrypted media

SIP devices can encrypt signalling and media, PSTN audio is only encrypted within the cloud (**unencrypted outside**)

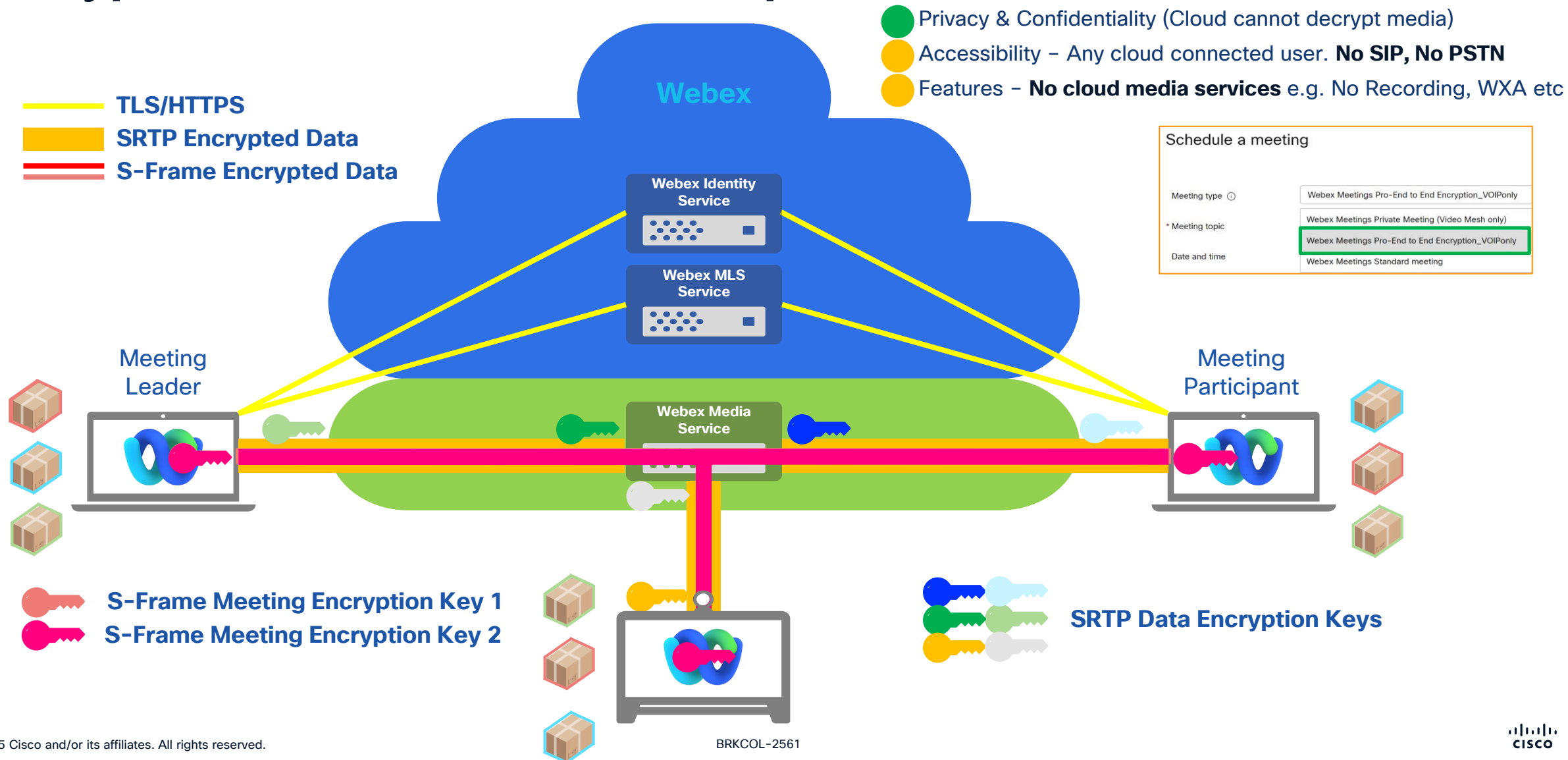
With standard Webex Meetings, the **cloud needs to access to encryption keys to decrypt SRTP media** from SIP devices, PSTN gateways and for other services such as recording

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)



Zero Trust Security for Webex Meetings – E2E Media Encryption MLS and SFrame operation



Zero Trust Security for Webex Meetings

Summary of E2E Encryption features

Supported:

End to End Encryption meetings are free for enterprise and consumer customers

Supported by Webex App (desktop and mobile) and RoomOS 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)

Not Supported:

Zero Trust E2EE = Webex has no access to meeting encryption keys

- Cloud services and endpoints that need to decrypt meeting content cannot participate in E2EE meetings:
 - PSTN and SIP endpoints
 - Cloud Recording
- Webex Assistant
- Meeting Transcription, Real-time translation, Closed captioning, Highlights
 - Web Browser based Webex App
- Older SX, DX, and MX series devices

Video Mesh

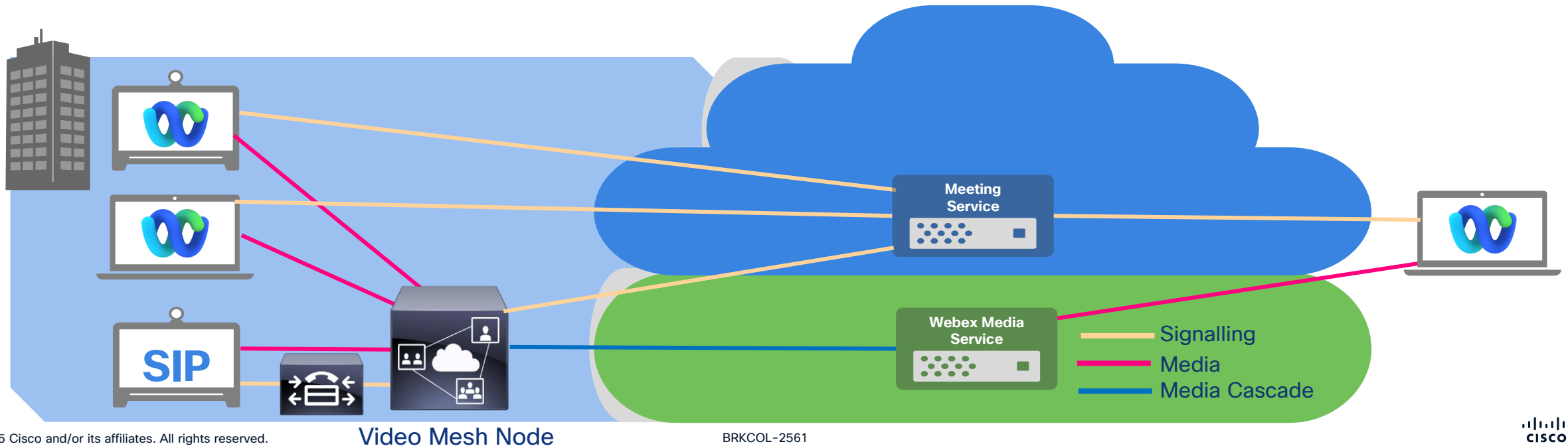
On-premises media termination for Webex Meetings and 1:1 Webex calls

Media cascades to the Webex cloud from Video Mesh

Off-network participants send media directly to Webex

All participants send signalling to Webex

Provides better performance, lower latency and internet bandwidth savings for on-premises participants



Private Webex Meeting

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 Cisco and 3rd Party SIP apps and devices may use encrypted signalling and encrypted media

Participants must be **Internal** and be **able to reach Video Mesh** (on-prem/within network boundary)

Schedule a meeting

Meeting type ⓘ

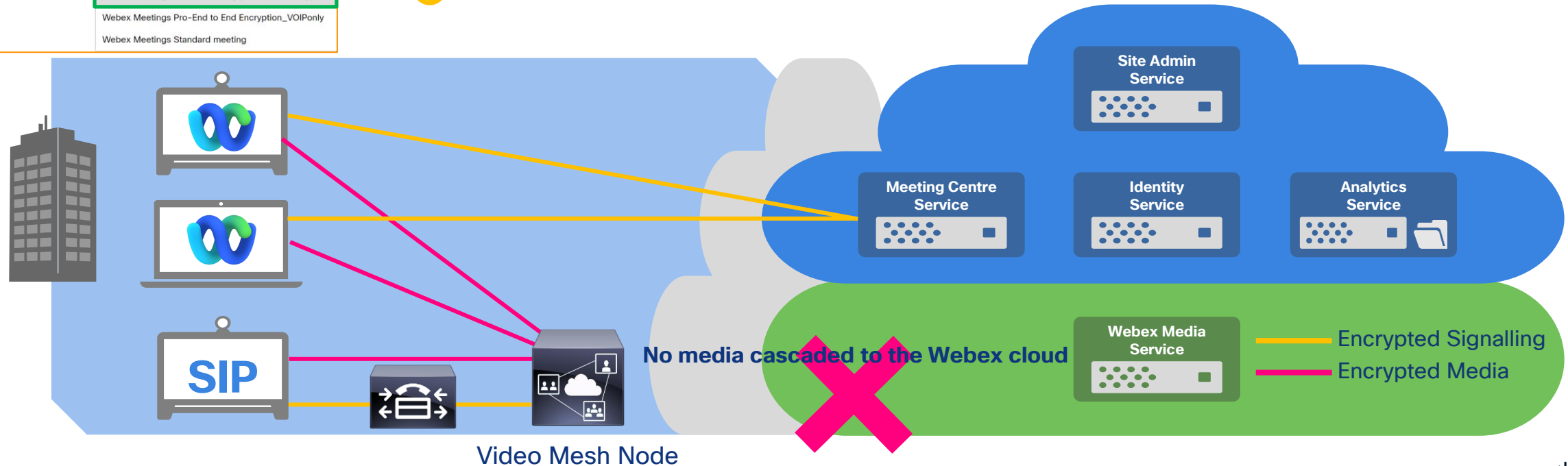
Webex Meetings Private Meeting (Video Mesh only)

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 (recordings, transcripts etc)



Webex Meetings : Lobby Controls and User Verification

Participants (12)

Kristine Stone is waiting in the lobby.

Internal • cisco.com

Let inRemove

Search

↓↑

In the meeting

Clarissa Smith

Host, me

Umar Patel

Presenter

Henry Riggs

...

🔇

Isabella Brennan

...

🔇

Kristin Stone

...

🔇

M

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

...

🔇

M

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)

Meeting Video & Roster Display : User Identity Information

Feature Planning Meeting

Host: Clarissa Smith

Copy meeting information

General

Security

Server connection

TLSv1.3 with ECDHE and AES-256-GCM

Media connection

AES-256-GCM

Secure encryption

Audio: **Yes**

Video: **Yes**

Screen and application sharing: **Yes**

Webex end-to-end encryption

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

Others (such as embedded Webex apps, embedded third-party apps, etc.): **No**

[Learn more about end-to-end encrypted connections](#)

Webex Meeting info

12:40

Layout

Smith

Henry Riggs (Unverified)

Brennan

Kevin Woo (example.com)

se Torres (Unverified)

Umar Patel (example.com)

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

G

Great Wall

Mute all

Unmute all

Mute

Stop video

Share

Record

Apps

Control Hub : Display/Hide Meeting participant labels

Webex Control Hub

Applies to all users in your organization

Default settings :

Unverified label = Displayed

Internal domain label = Hidden

External domain label =
Displayed

Some organizations find the Unverified label distracting e.g., In Public/ Town Hall meetings where many participants do not have an account/ have not signed in

Meeting

 Sites

 Settings

 Manage Meetings and Webinars

 Templates

User labels

For security reasons, Webex marks participants with an **unverified** label if they aren't signed in or if we can't confirm their identity. For more help, [see how the unverified label works in meetings](#) 

 Show the unverified label in meetings

Verified users can receive a **domain** label to display their domain or company when joining meetings. For larger meetings, this label can help quickly identify other participants that aren't in your org. For more help, [see how the domain label works in meetings](#) 

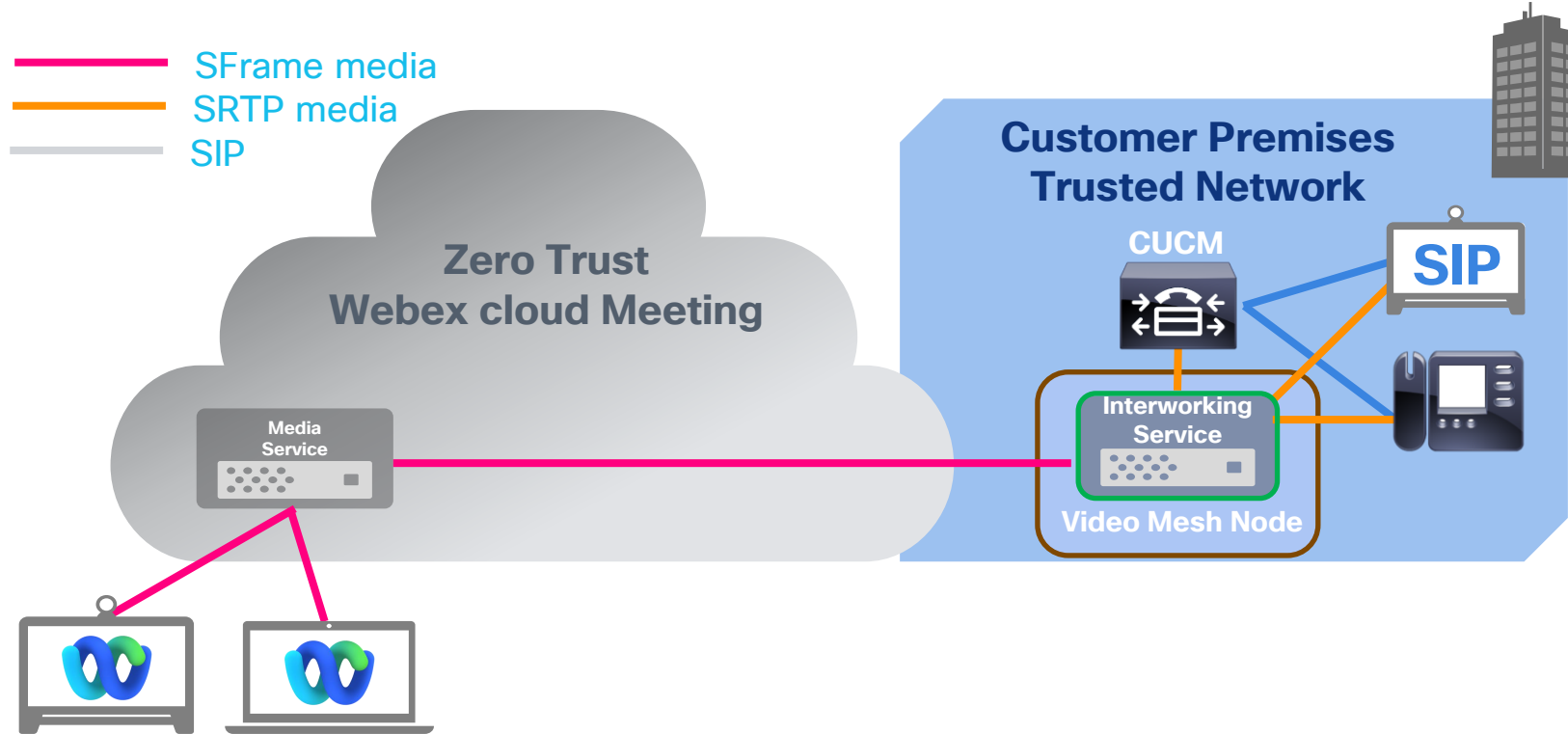
 Show the domain label for users from my organization

 Show the domain label for external users

Extending Zero Trust and End to End Encryption

Webex E2E Encrypted Meetings with Trusted On Premises Participants

Roadmap



Internal and External participants can join E2EE meetings via the Webex App or Cisco Video devices

ALL users on the hosting organization's trusted network can join Zero Trust Webex Cloud E2EE'd meetings....

Internal user dials 1-800-Webex...

- Redirect SIP call to VMN
- Encrypted media on Premises
- E2EE'd media in Webex Cloud

E2E Encryption Only in the Webex Cloud & Video Mesh Node

Video Mesh Node with SIP Trunk to CUCM

Video Mesh Node with customer managed public CA signed cert

Trusted on premises SRTP endpoints joining cloud E2EE'd meetings

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

The screenshot displays a Webex meeting interface. On the left, a sidebar titled "Feature Planning Meeting" shows the host as Clarissa Smith and a "Copy meeting information" button. Below this, the "Security" tab is active, displaying connection details: "Server connection: TLS with ECDH and AES-256-GCM", "Media connection: AES-256-GCM", and "Zero Trust end-to-end encryption" with "Audio: Yes", "Video: Yes", and "Screen and application sharing: Yes". It also lists "Chat, files, whiteboards, and annotation: Yes" and "Others (such as embedded Webex apps, embedded third-party apps, etc.): No", with a link to "Learn more about end-to-end encrypted connections".

The main area shows a 3x2 grid of video thumbnails for participants: a Smith, Henry Riggs, Isabelle Brennan, Kevin Woo, Marise Torres, and Great Wall. The bottom of the interface features a toolbar with buttons for Mute, Stop video, Share, Record, and other controls. On the right, a "Participants (6)" list shows the names and email addresses of the participants, including Clarissa Smith (Me, host), Kevin Woo (Presenter), Henry Riggs (Unverified), Isabella Brennan, Marise Torres (Unverified), and Great Wall.

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

User's Verifiable Credential generated by GoDaddy CA.
Select the icon to view the credential details.

Clarissa Smith

Me, host • company.com

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

Henry Riggs

Unverified

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

Great Wall's Verified Credentials

GoDaddy Certificate Authority

GoDaddy Certificate Authority

*****@example.com

This identity credentials are valid.

Subject

user: b3ece9e9-6168-4cda-9265-0c76...

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's Verified Credentials

Webex Certificate Authority

Webex Certificate Authority

*****@company.com

This identity credentials are valid.

Subject

user: b3ece9e9-6168-4cda-9265-0c76...

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's Webex Verified Credentials

Webex Certificate Authority

Webex Certificate Authority

(No identity)

This certificate is valid.

Subject

anonymous: b3ece9e9-6168-4cda-926...

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 Deepfake Detection

Beta

Webex is partnering with Pindrop to deliver Deepfake detection in Webex Meetings

Add Pindrop Pulse to Webex (Pindrop license required)

Apps

pindrop

Search result for 'pindrop'

Pindrop

Pindrop Pulse for Meetings

Detect Deepfake Threats

Webex Meeting info Show menu bar

Chelsey Krull

Layout

Security Assistant is recording this call

Mute Stop video Share Record

Pulse for Meetings

Back to list

Alerts (1)

Chelsey Krull

Analyzed speech 00:00:06

Audio analysis Synthetic

Video analysis Synthetic

Reset analysis

Analyzed participants (1)

Sarosh Shahbuddin

Stop analysis

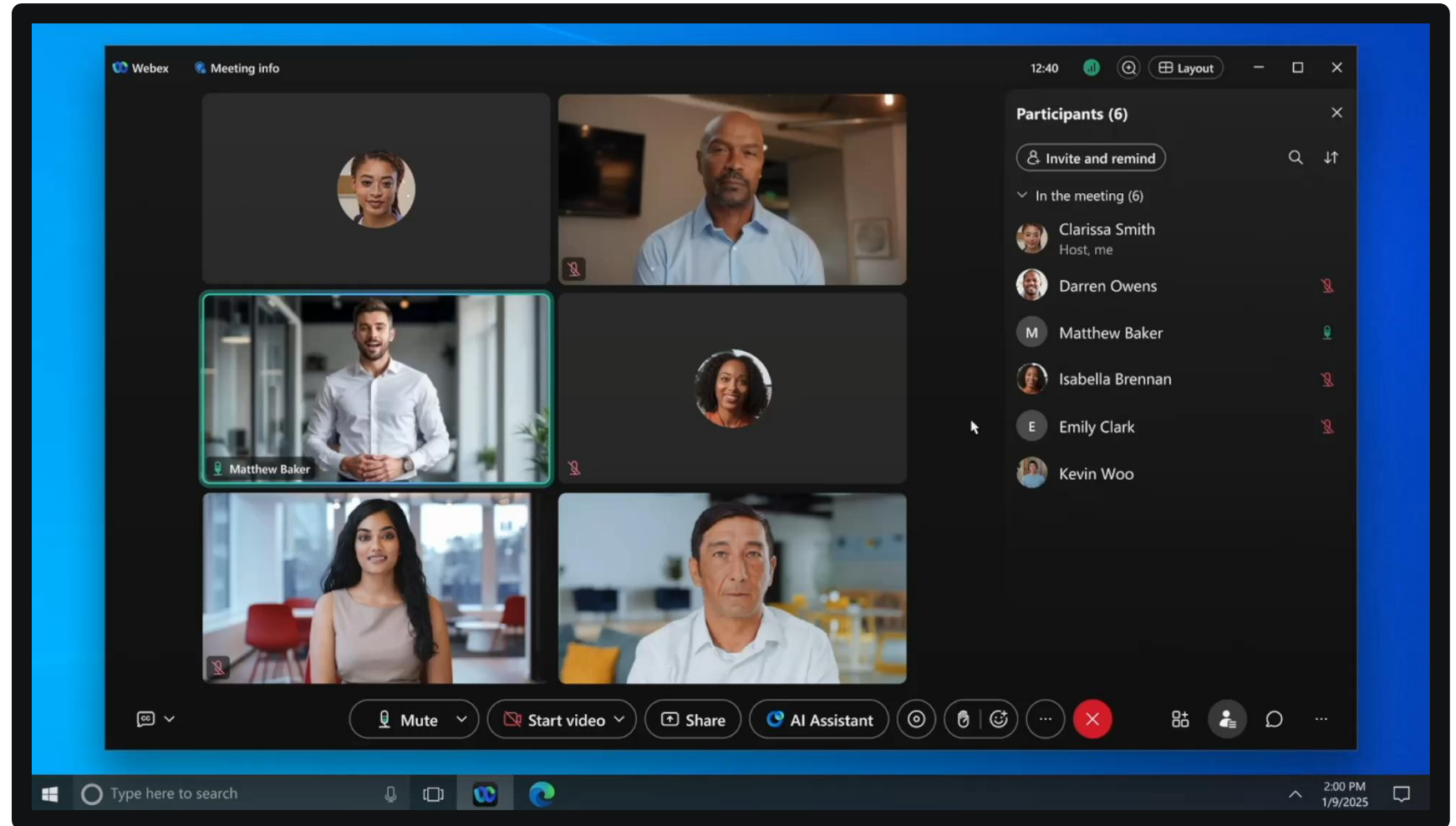
View more details



Deepfake Detection – Native Integration

Roadmap

Roadmap to more natively integrate deepfake detection capabilities into Webex



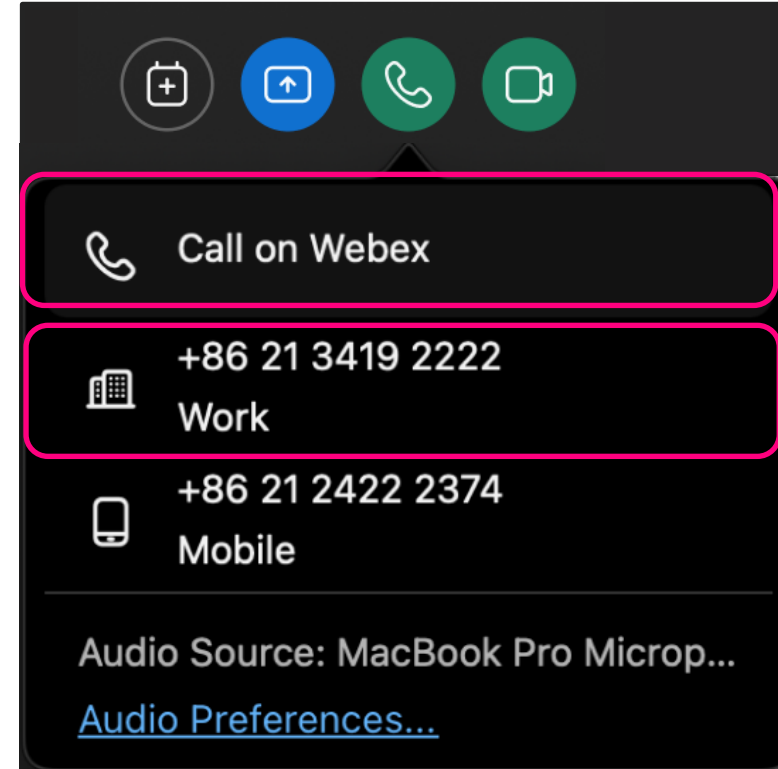
New Feature - E2E Encrypted Calls with Webex Calling

Webex App E2E Encrypted 1:1 Calls

- Call on Webex
- Webex Calling

Today: Webex App (Desktop, Mobile)

Planned: Devices



E2E Encrypted calls – Call on Webex

Organization wide setting in Control Hub

When enabled – all calls will attempt to set up End to End Encryption

No user intervention required :

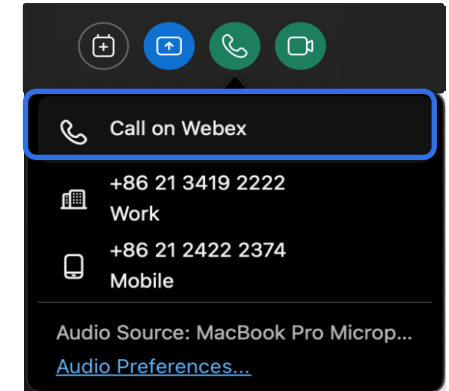
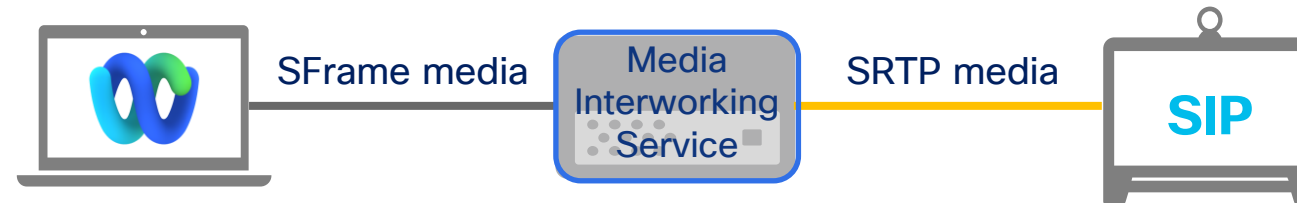
If all endpoints support E2EE (MLS & SFrame)

=> Call is E2E encrypted

If one endpoint supports does not support E2EE

=> Call uses standard SRTP encryption

Participants informed of change in security state via onscreen notifications



To support SRTP endpoints, Webex provides an SFrame to SRTP media interworking function

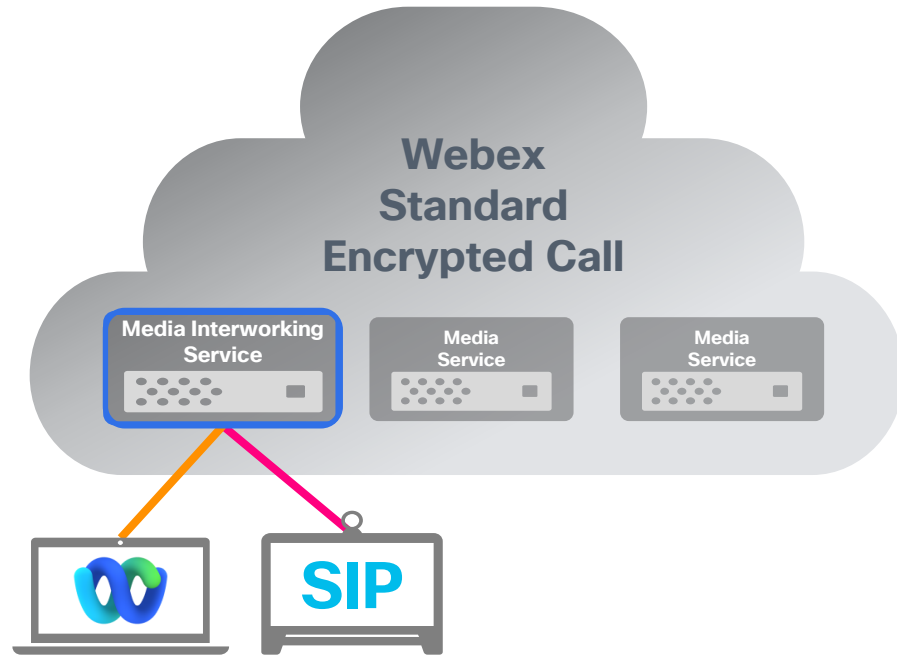
MLS group and SFrame maintained for endpoints that support E2EE.

E2E Identity maintained for MLS users – Identity verification prevents Deepfake attacks

Webex Standard Encrypted Call

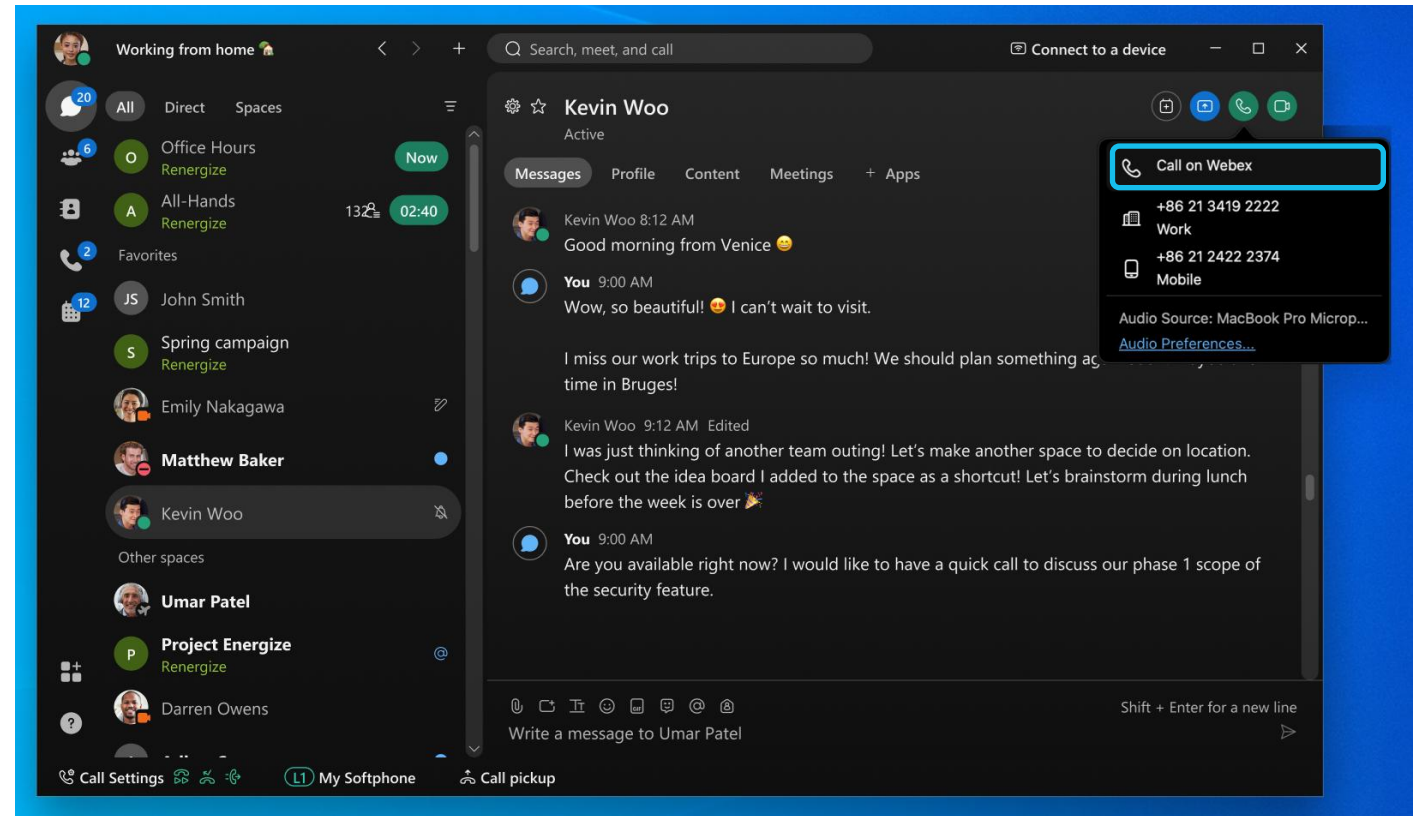
Webex App supports E2E Encryption

SIP device does not support E2E Encryption (SRTP Only)



— SRTP media
— SFrame media

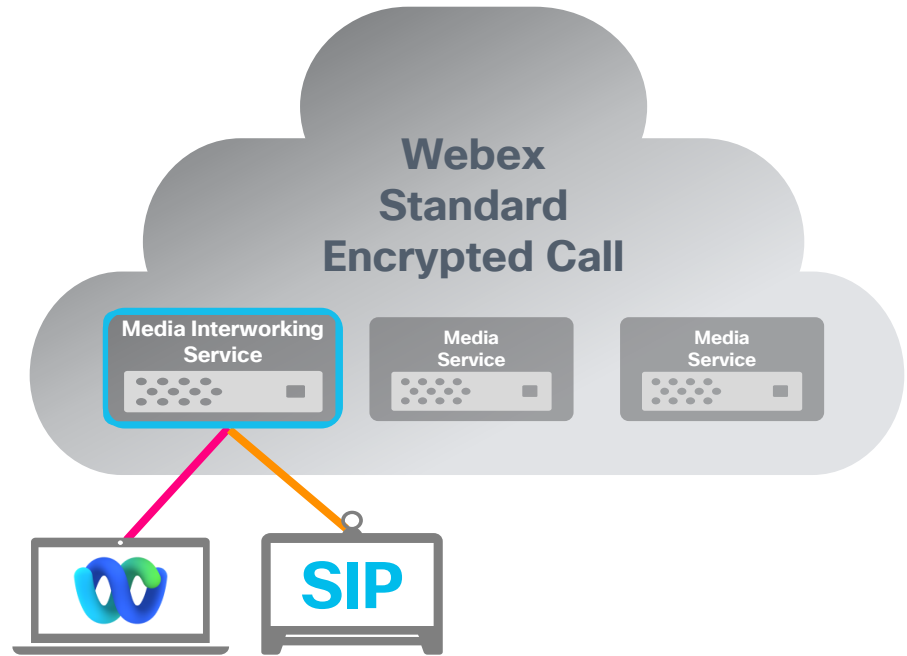
Clarissa Smith calls Kevin Woo



Webex Standard Encrypted Call

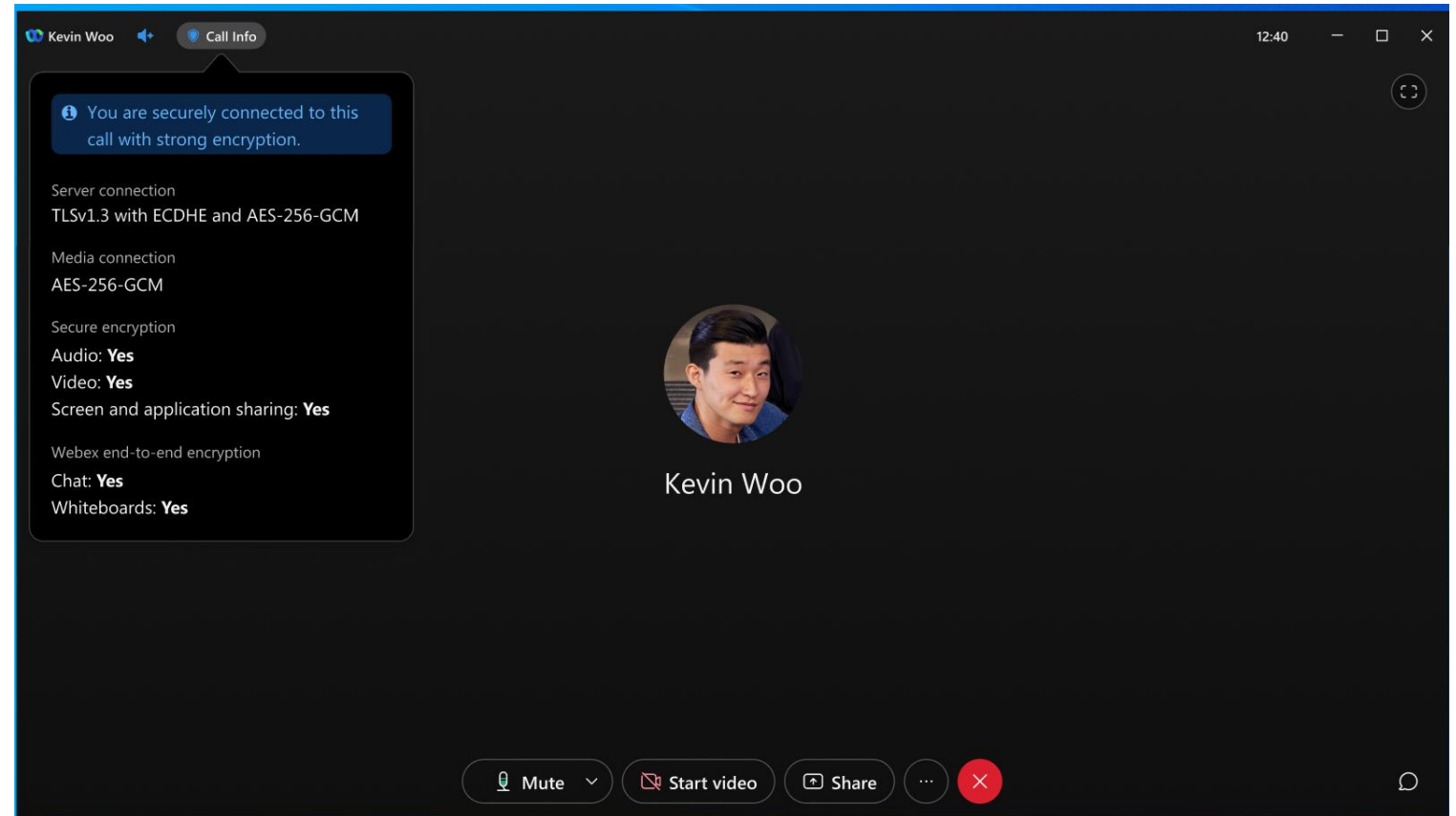
Webex App supports E2E Encryption

SIP device does not support E2E Encryption (SRTP Only)



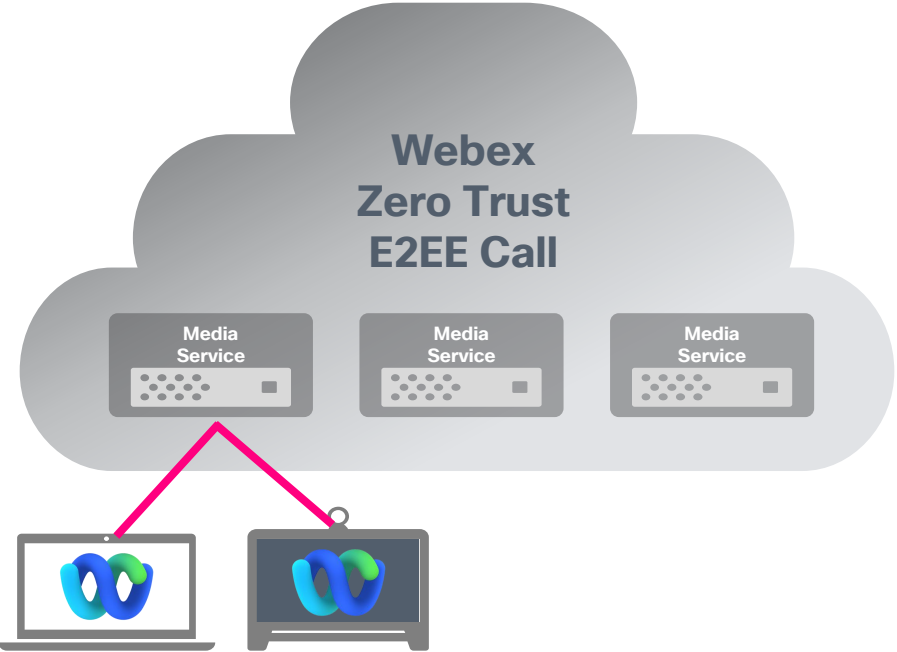
— SRTP media
— SFrame media

Clarissa Smith calls Kevin Woo



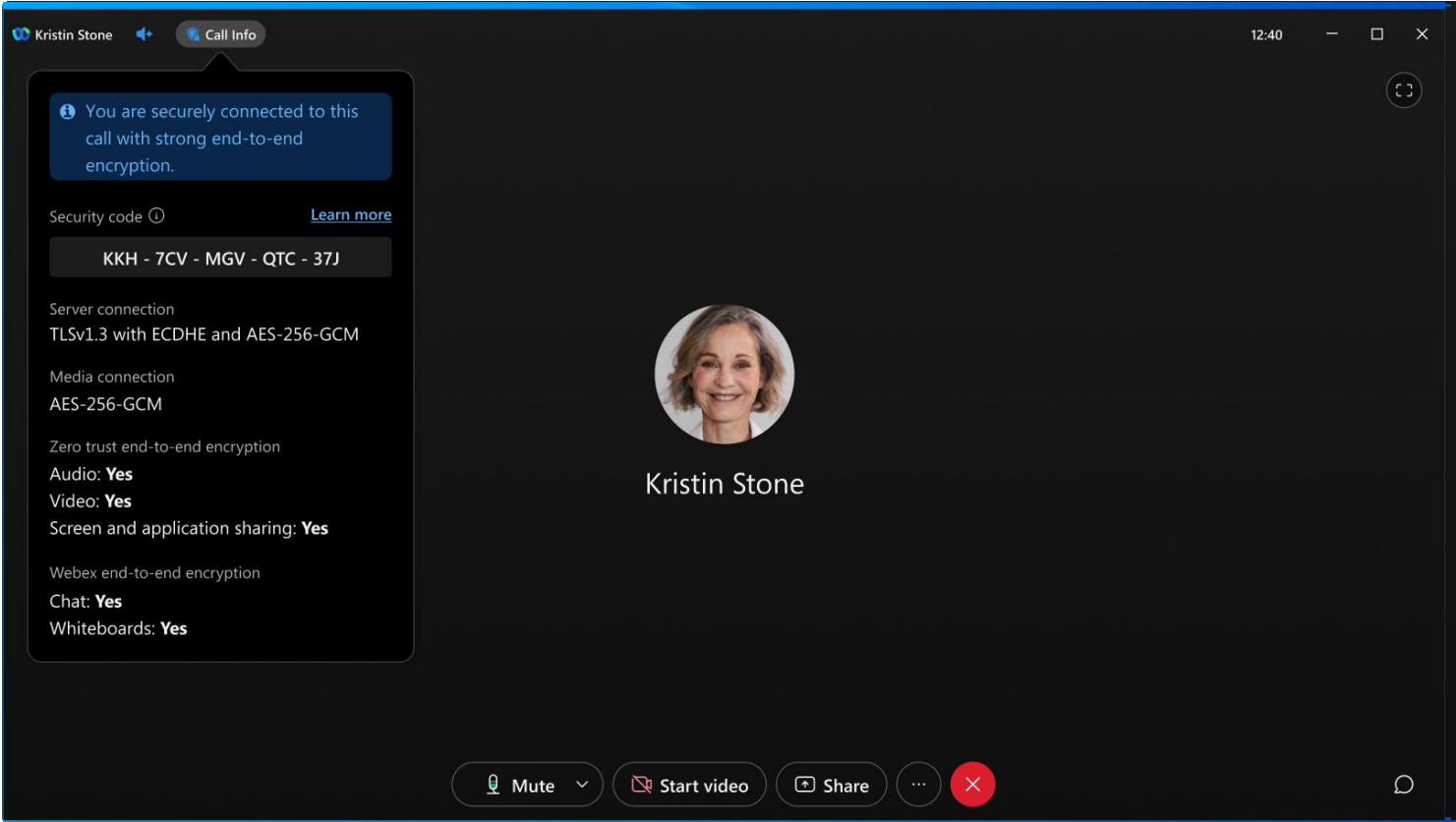
Webex End to End Encrypted Call

Webex App and Webex Device both support E2E Encryption



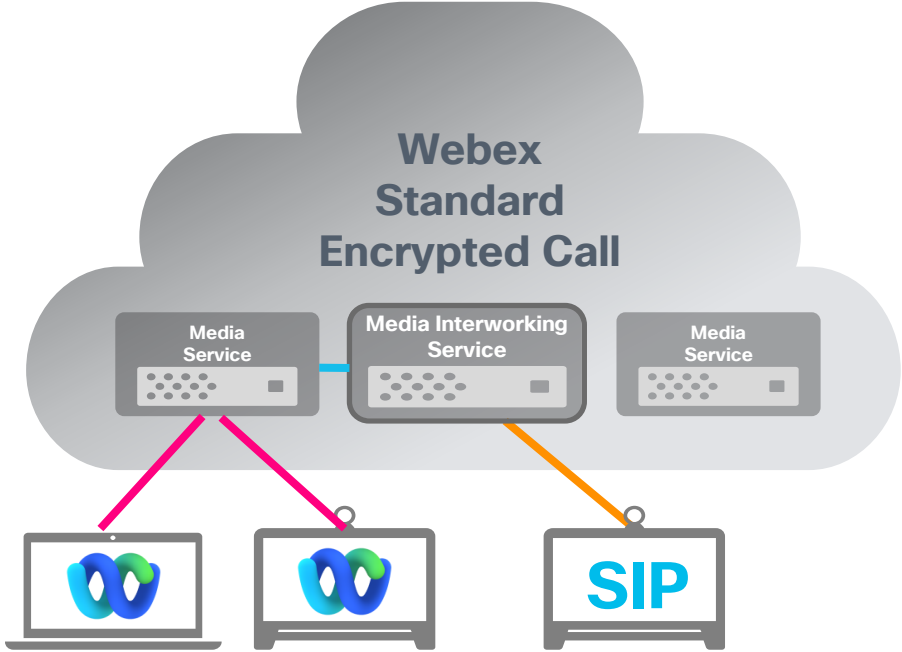
SFrame media

Clarissa Smith calls Kristin Stone



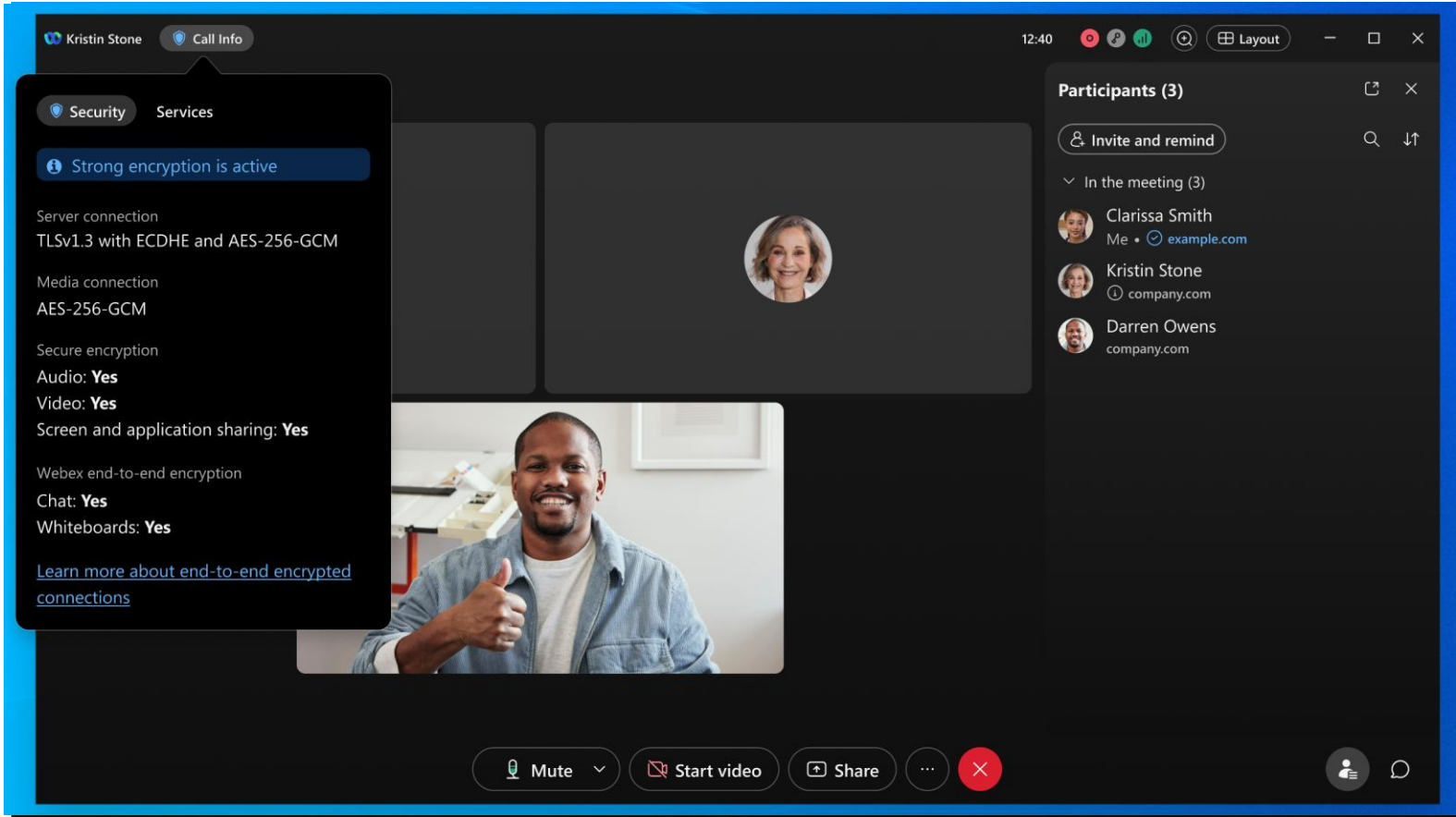
Webex E2EE Call Downgrades When SRTP Participant Added

Webex App And Webex Device Both Support E2E Encryption
New Participant Does Not Support E2EE (SRTP Only)



— SRTP media
— SFrame media

Clarissa Smith adds Darren Owens to the call



Post Quantum Resistant Crypto

Post Quantum Resistant Cryptography

Webex uses PQ resistant ciphers today for media and signaling
AES-256-GCM – preferred cipher for signaling and media

PQ resistant ciphers needed for key negotiation

Three phases of PQ support

- 1) Webex adoption of CiscoSSL version with PQ support
 - Provides support for TLS with PQ resistant key negotiation
- 2) Webex adoption of PQ resistant key negotiation for signaling to Webex KMS
 - Provides PQ resistant signaling encryption for user generated content (chat, files etc)
- 3) Webex adds support for PQ resistant deterministic key generation fo MLS
 - Provides PQ resistant key negotiation for media and content shared in E2EE'd Meetings

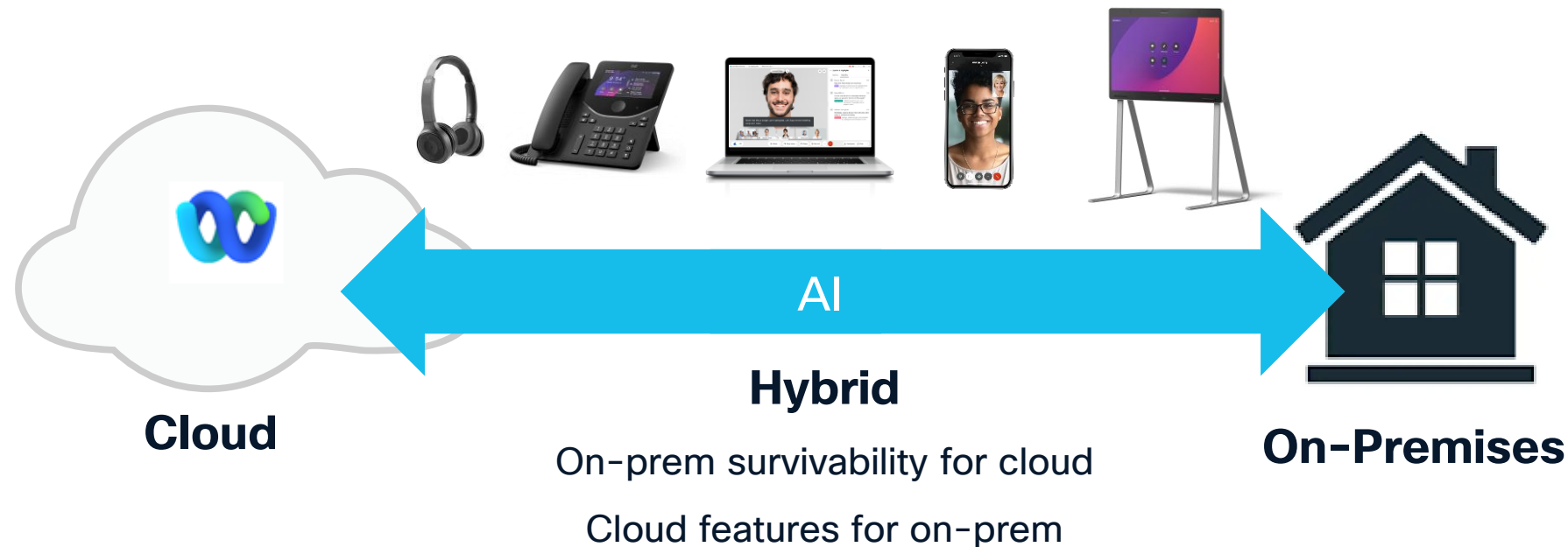
Digital Resilience for Collaboration

Digital Resilience

Digital Resilience is the ability of an organization to keep its business securely up and running despite any disruption.

For **collaboration technologies**, this can mean:

- keeping critical services running in spite of network, cloud or service disruptions
- providing additional assurance or higher security posture to your communications and data
- Extending cloud and AI capabilities to resilient on-premises deployments

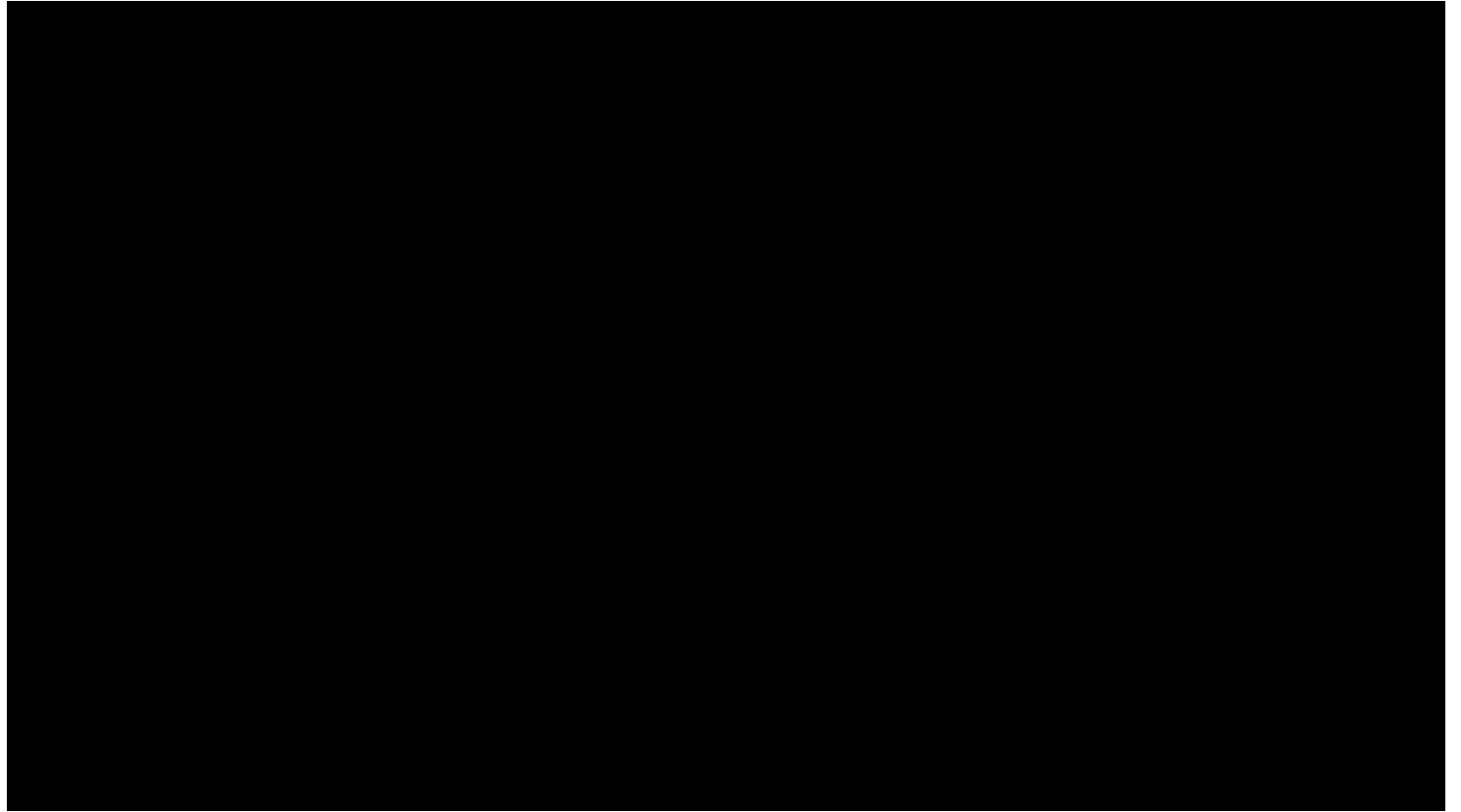


Packet Loss – Audio Disruption in Calls and Meetings

It's very common for users to experience packet loss or poor network conditions, even during day to day use

The likelihood of these incidents can increase during emergencies – network interruptions, congestion

These are often when it's most critical to be able to communicate clearly



Audio Resilience with Webex AI Codec

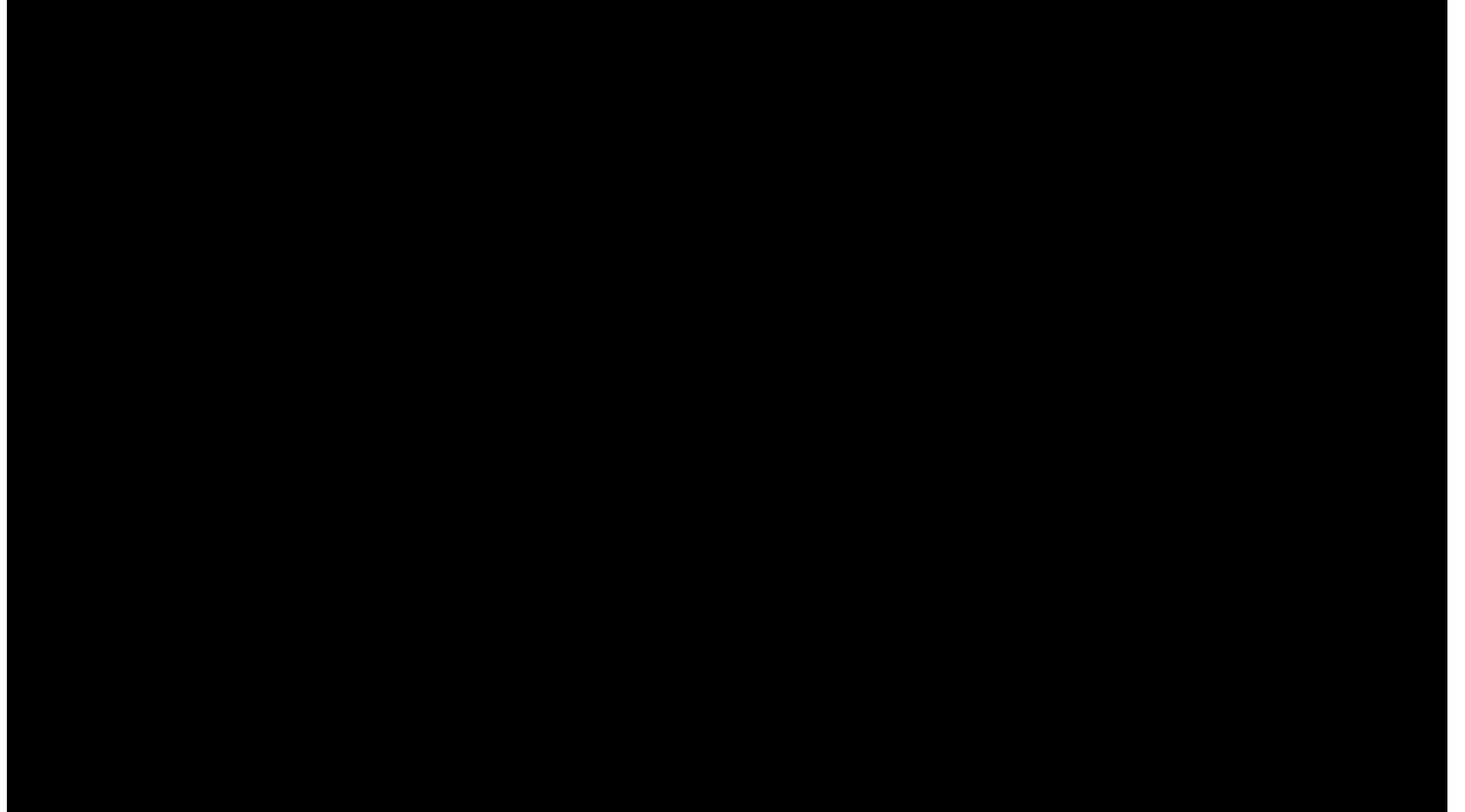
Webex AI codec uses advanced encoding, decoding and AI to reduce bandwidth usage and provide high audibility at up to 80% packet loss

Supports Webex Calling 1:1 and Webex Meetings between compatible devices (Webex App – desktop and mobile)

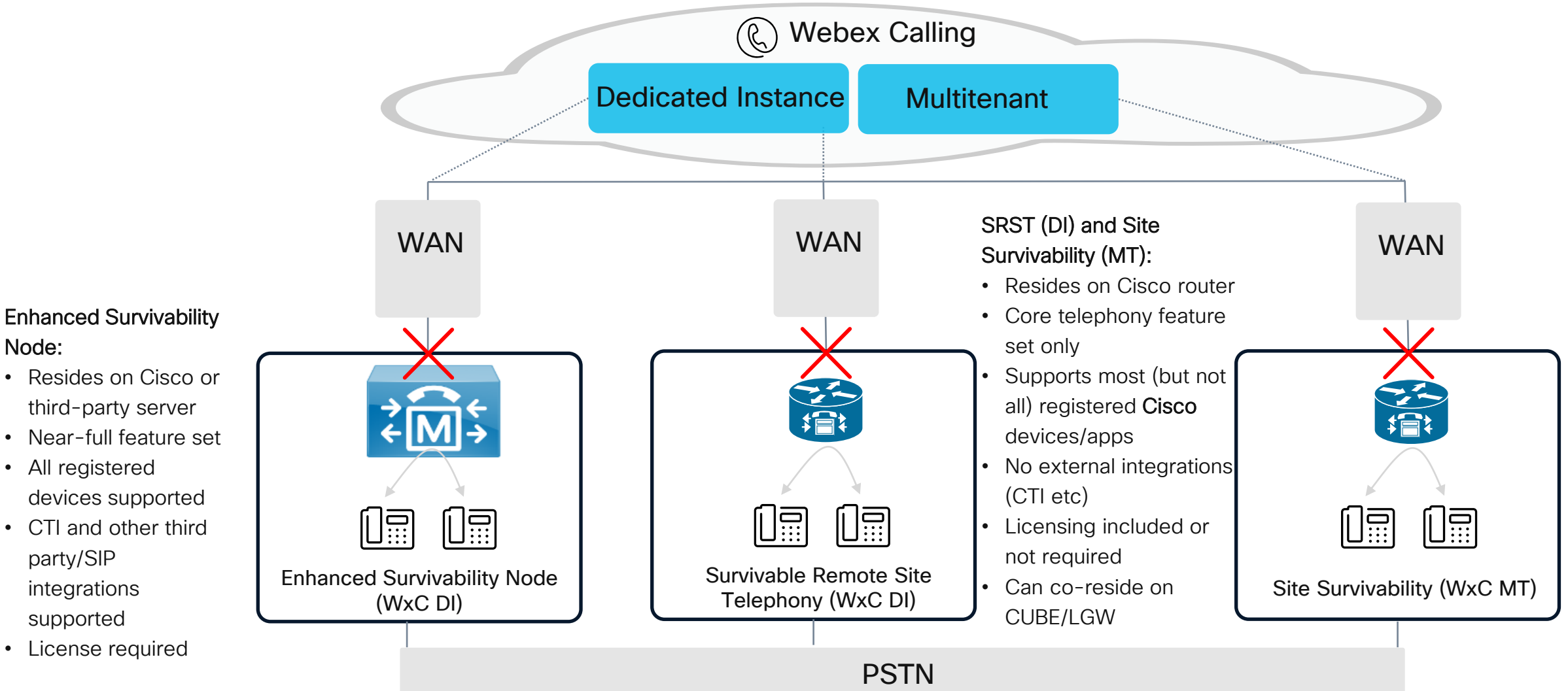
Calls and Meetings automatically switch to AI codec when packet loss detected

Roadmap:

Transcode for non-compatible devices, CUCM support



Webex Calling – On-Prem Survivability Options



Cloud Connected UC

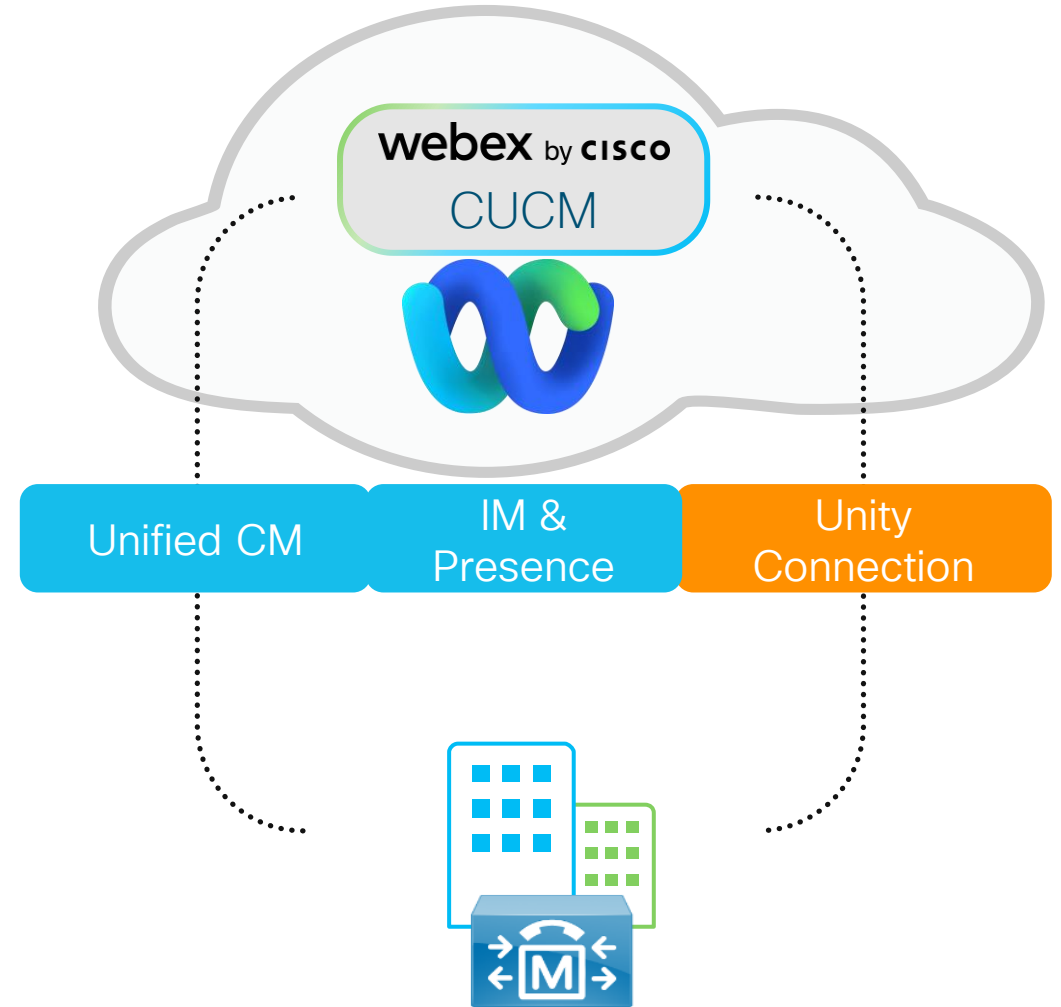
Cloud Benefits, On-Prem Resilience

Use Cloud Connected UC to deliver cloud features to on-premises UCM deployments

Maintain full, customer controlled on-premises telephony deployment with no dependency on cloud for core services

Leverage Cloud For:

- Webex directory/user sync (including from Entra ID/SCIM etc)
- Presence sync (including to MS Teams w/ Cisco Calling integration)
- Cloud management – dashboards, analytics, certificates, WebRTMT



Webex Calling Hybrid

Extending cloud capabilities to on-premises UCM deployments

Roadmap

Coming Soon:

Leverage key value-adds from Webex Calling while keeping core telephony on-premises with CUCM



AI cloud innovation

AI Receptionist
Customer Assist



Cloud administration

Control Hub
Call recording



Cloud trunking

Cloud PSTN
Cisco Calling Plans
Third party integrations

Cisco Calling for Microsoft Teams

With CUCM or Webex Calling

Call history and voicemail

User presence sync MS <> Webex

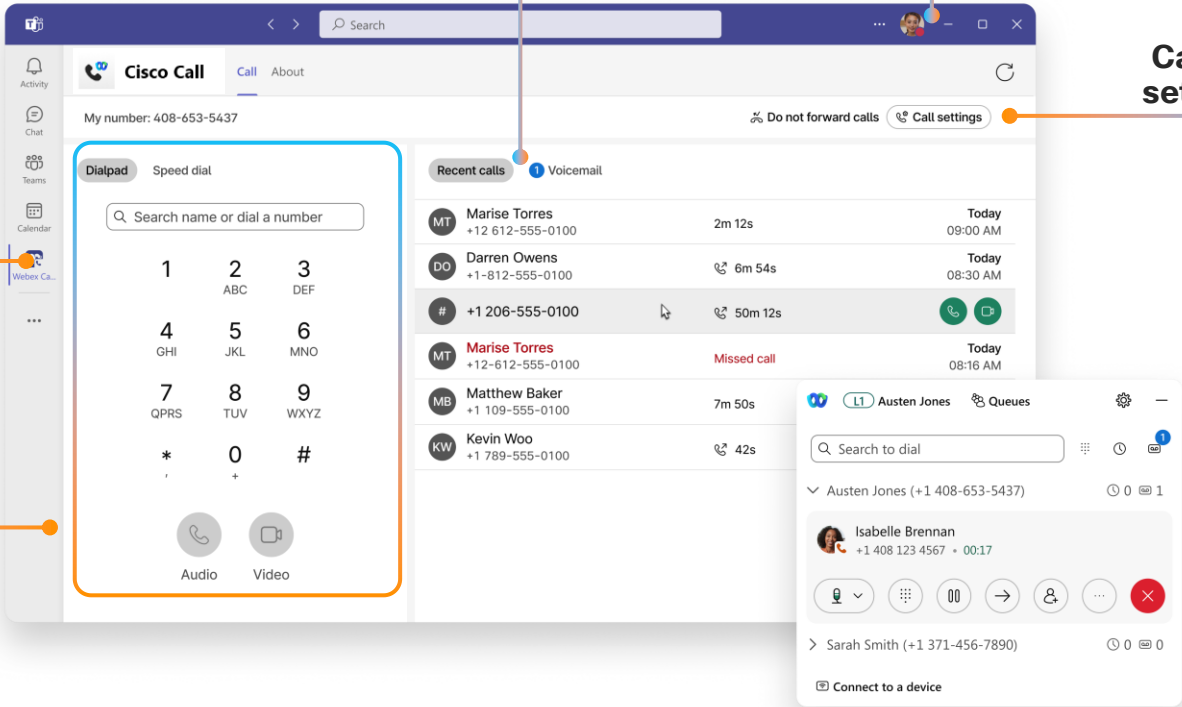
Calling settings

One click Cisco Calling access from Teams sidebar

Dialpad + speed dial
Dial by extension, number, directory search, or saved speed dial contacts

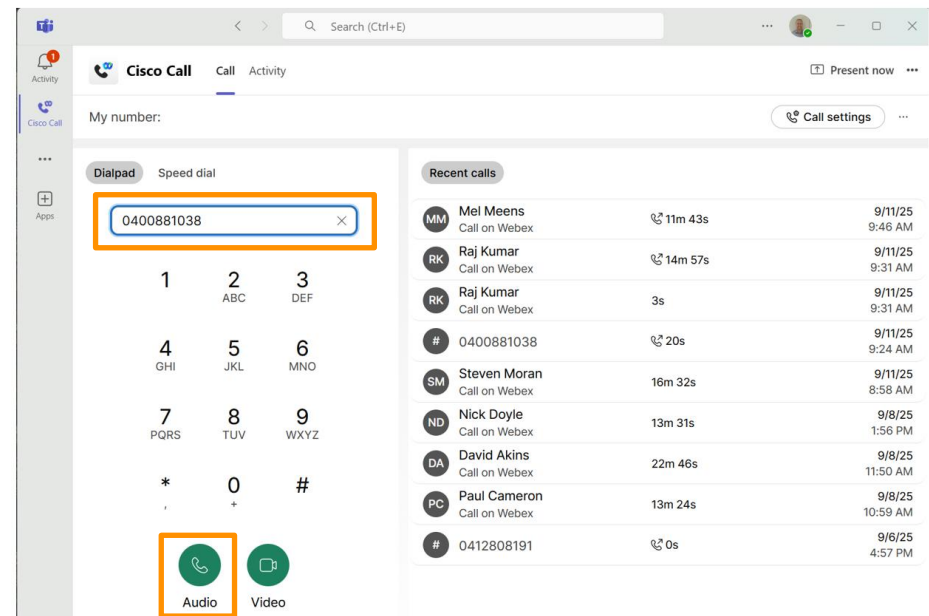
Multi call window
Enables Teams users to select from multiple lines, join / unjoin queues

Desk Phone Control
Launch calls from your desk phone

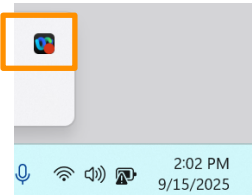


Cisco Calling for MS Teams – Normal Operations

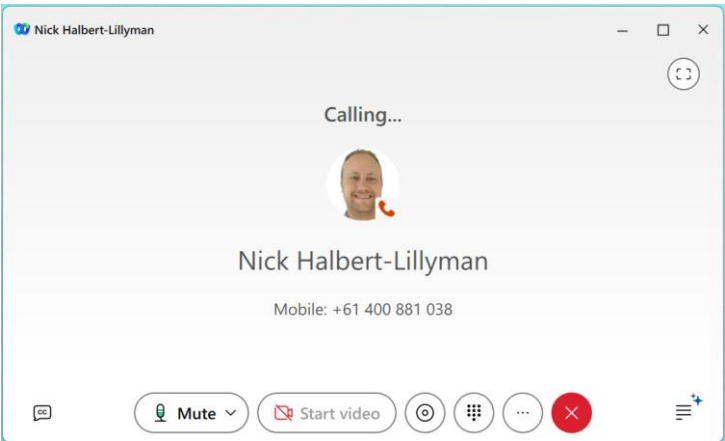
User places call from within Teams – Cisco Calling tab



Webex App:
Optionally Hidden in System Tray



Launches call from Webex App window (pops up from System tray)



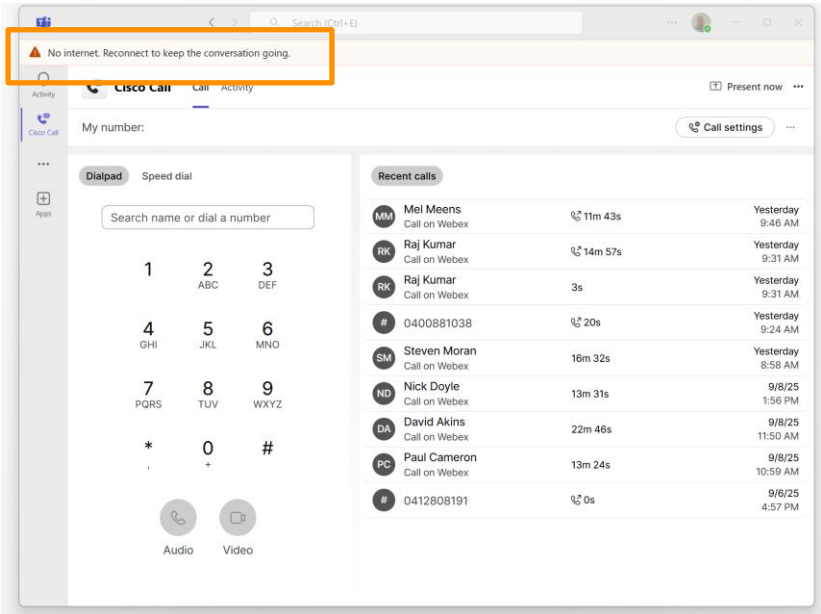
Or launches call from Desk Phone (if Desk Phone control is set)



Cisco Calling for MS Teams – Teams/Internet Outage

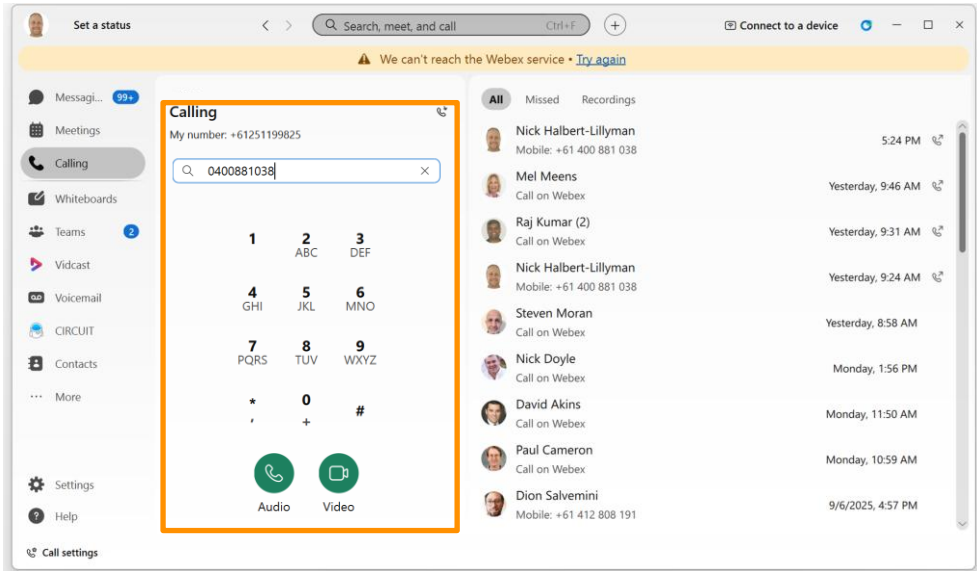
With CUCM or Webex Calling w/Survivability

Internet Outage – Teams Offline

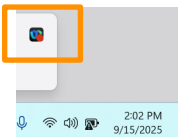


Calling still available from Webex App or Desk Phone,
other Webex Services unavailable

(Local CUCM *or* Webex Calling Survivability)



Desk Phone continues
as normal (CUCM) or
displays “Limited
Features” warning
(Webex Calling)



Note:
Open Webex App from system tray if configured as hidden

Webex Meetings with Trusted On Premises Recording

Currently in Beta

<https://gobeta.webex.com>

Video Mesh Node with Recording Service

Trusted on premises Recording Service
joining Webex meetings

Meeting Recordings stored on premises
customer provided NFS share
Native Webex recording UI

Use Cases

Legal/Courts

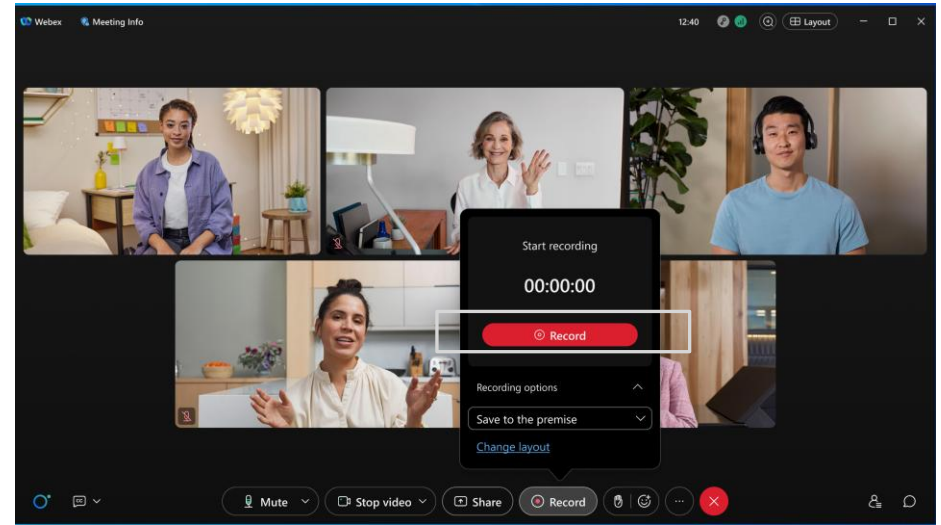
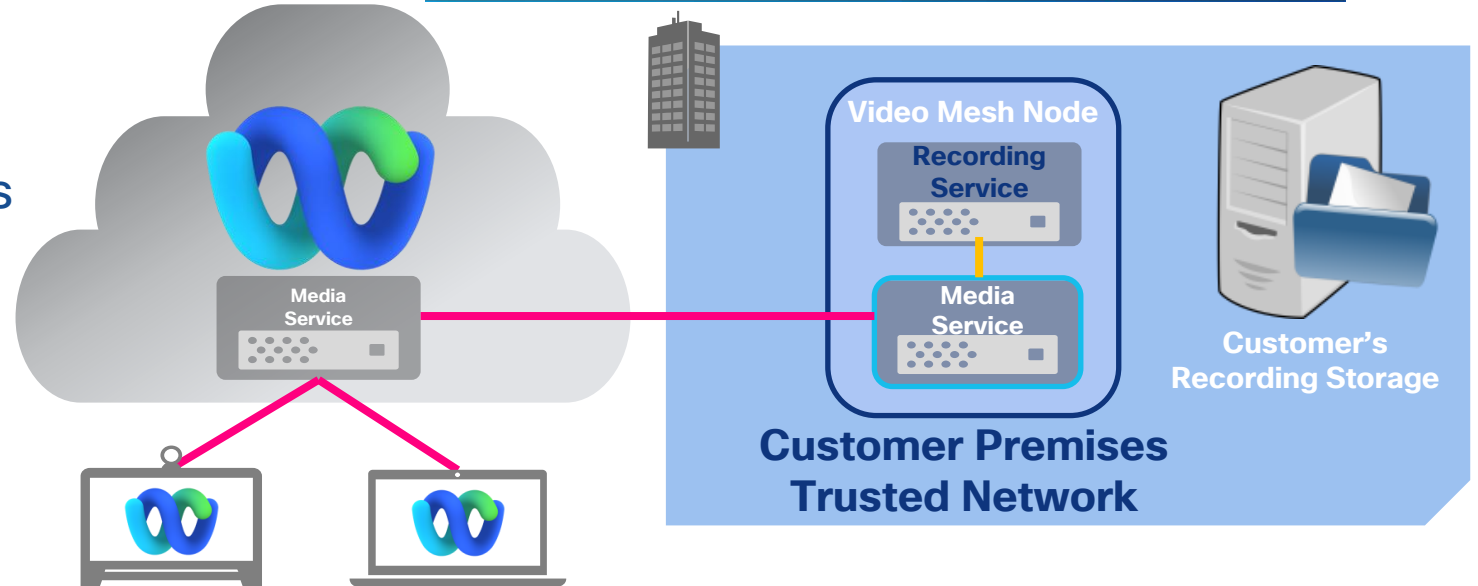
Jurisdictional Data Storage Requirements

Long retention (over 10 years)

Highly critical or sensitive data

In Development

On-prem recording for Zero Trust E2E
Meetings – Video Mesh as E2E Gateway



Collaboration AI Pods

Roadmap – final scope TBA

Leverage Cisco AI pods to deliver AI-driven collaboration capabilities internally, for cloud and on-premises meetings

On-Prem/Air-Gapped

Deliver AI capabilities to on-prem Cisco Meeting Server – no cloud connection required.

Proposed capabilities:

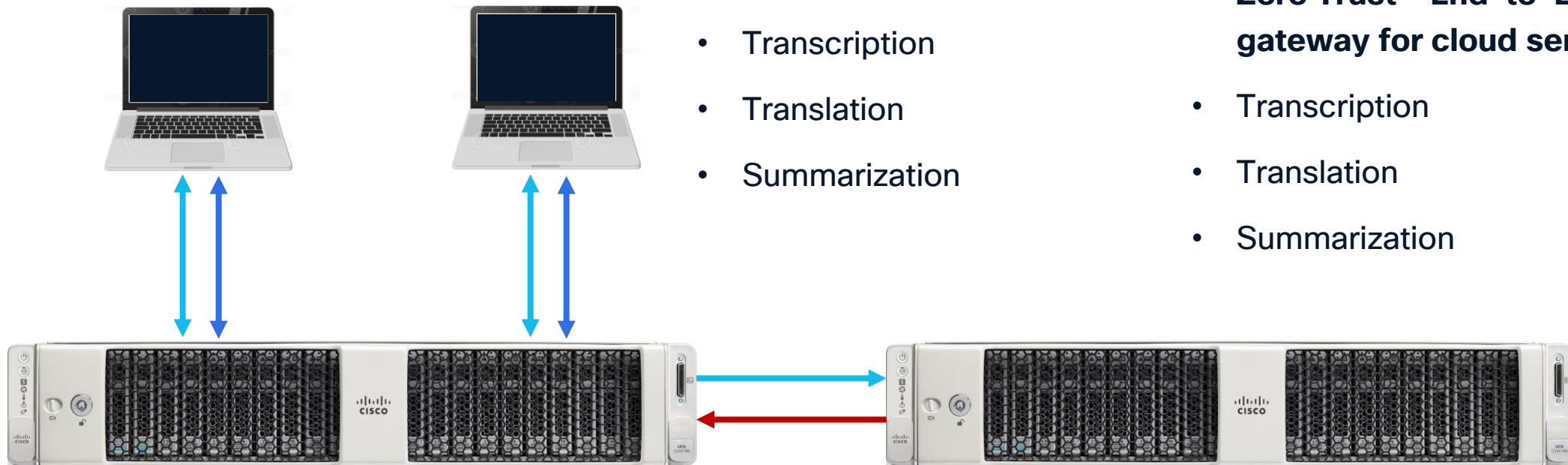
- Real-Time Closed Captioning (committed)
- Transcription
- Translation
- Summarization

Webex w/Video Mesh

Deliver AI capabilities to Webex Meetings from on-prem infrastructure, for hyper-secure meetings.

Proposed Capabilities:

- Managed via Webex Control Hub
- **Zero Trust - End-to-End Encrypted gateway for cloud services**
- Transcription
- Translation
- Summarization



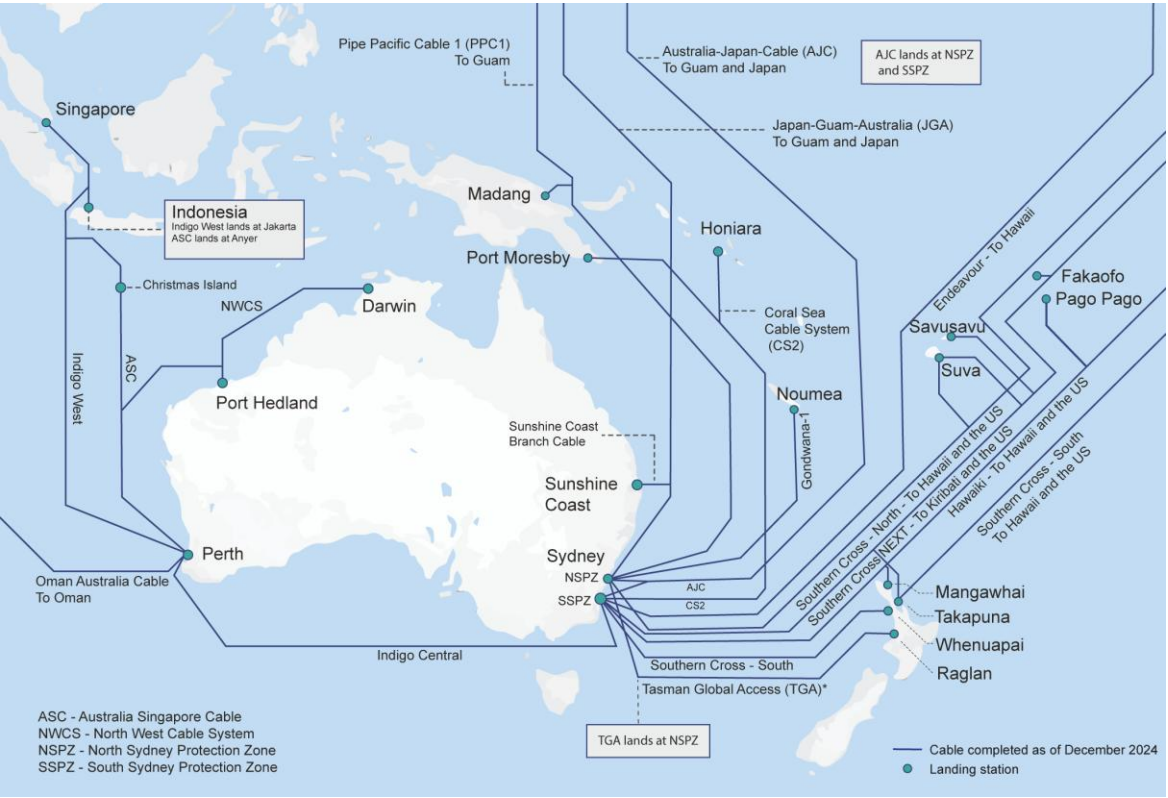
Cisco Meeting Server (CMS) or Video Mesh

Cisco AI Pod

Webex Australian Data Residency and Compliance

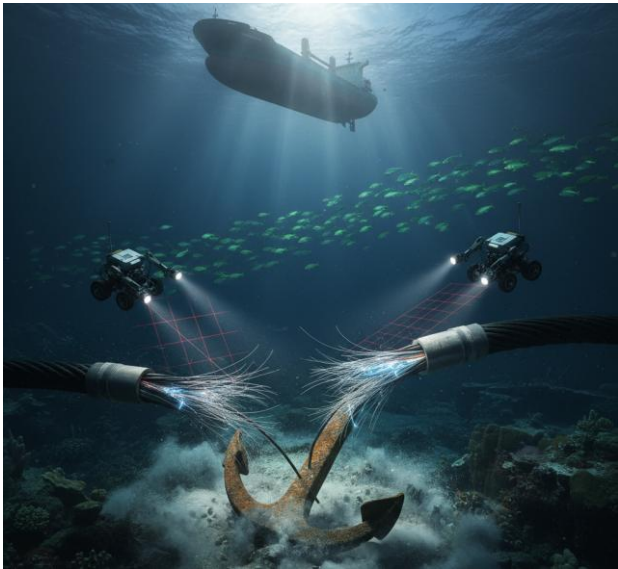
Our Home is Girt By Sea....

...and undersea cables.



Australian Communications and Media Authority © Commonwealth of Australia.

These links can be disrupted by ships dropping anchor, natural disasters...



Congestion, routing issues...



Or Sabotage.



Webex Suite: Australian Data Residency

- Webex already has a substantial on-shore presence in Australia – Meetings (single DC) Calling, Contact Center, CPaaS
- Cisco is bringing remaining Webex services to Australia, including Messaging, Identity, Slido, Common Identity, Secondary Meetings DC
- This enhances Webex resiliency for Australian customers and provides assurance for customers with on-shore data residency requirements



Webex Suite: Australian Data Residency

Today – Onshore Services



Calling



Meetings (Primary DC)



Contact Center



Webex Connect – CPaaS

Coming Soon!



Meetings (Secondary DC)

Media DC – Nov CY25

Other Meeting Services – Feb/Mar CY26



Messaging Nov CY25

Inc Hybrid Calendar, Device Reg, in-meeting chat



Slido (via Webex Control Hub)– Nov CY25

*meetings integration Feb/Mar CY26



Analytics & Reporting – Feb/Mar CY25



Identity – Feb/Mar CY25

Australian Data Residency – Availability and Migration

Webex Meetings:

Current backup site for ALL Australian Webex customers (storage of recordings/transcripts, meeting orchestration etc) to be moved to secondary AU DC (Melbourne) – transparent to customers

New Media DC – can be used by any Webex participant at launch (Webex Meetings participants always use closest DC)

Other Services:

Available for new customers at launch date.

Migration for existing customers – work with Cisco account team

Webex IRAP Assessment for Australia

IRAP assesses security controls for a system (e.g. Webex) against documented security controls from the Australian Government Information Security Manual (ISM), published by the Australian Signals Directorate (ASD)

Targets security controls at a certain security level (e.g. OFFICIAL, PROTECTED etc). Especially relevant to public sector organizations

Webex IRAP Assessment @ PROTECTED includes Webex Meetings, Messaging, Calling, Control Hub.

Webex Contact Center IRAP in-progress.



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



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

Contact me at: Webex/Email nhalbert@cisco.com

Thank you

CISCO Live !

