
cisco Live!
ALL IN

The bridge to possible

Collaboration Security and Cloud Transitions

Matt Jordy, Technical Marketing Engineer, CTG
@jordy_cisco / mjordy@cisco.com

BRKCOL-2895

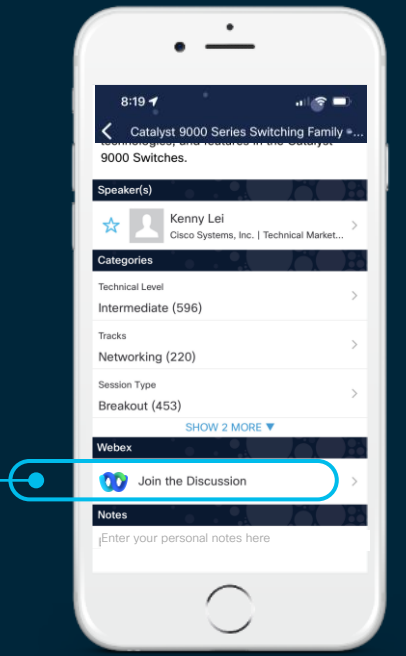
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2895

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda

- Introduction
- Migration Use Case
- Privacy and Data Residency
- Identity and Auth(entication/orization)*
- Encryption and Network Considerations
- Compliance and Data Control
- Conclusion

* AuthN = Authentication / AuthZ = Authorization

Collaboration Security

Privacy

What? / How long?

Identity

Verified?

Encryption

Encrypted? / How?

Compliance

Compliant?

Certified by
3rd party?

Logistics

- This is a 45-minute session, so we have limited time for both content and Q&A.
- We'll stop a few places along the way to handle 1 or 2 questions.
- It's very likely we won't be able to get all the questions in the allotted time. If we don't get to your question:
  - » See me after the session
  - » Put your questions in the Webex space for this session
  - » Send me a 1:1 Webex message or email (mjordy@cisco.com)

Logistics

- This is a 45-minute session, so we have limited time for both content and Q&A.
- We'll stop a few places along the way to handle 1 or 2 questions.
- It's very likely we won't be able to get all the questions in the allotted time. If we don't get to your question:
  - » See me after the session
  - » Put your questions in the Webex space for this session
  - » Send me a 1:1 Webex message or email (mjordy@cisco.com)

Here Today, Gone Tomorrow

Refer to the latest documentation for the most up-to-date information on supported features, best practices, and platform operation.

- Cloud software changes: how it is configured, where it is located, and sometimes even how it operates. (On-premises software changes too)
- People make mistakes, certificates expire, defects happen, updates occur, products end-of-life, new integrations are required, …

Migration Use Case

Collaboration Deployment: On-Premises

ON-PREMISES

MEETINGS

Meetings
(Cisco Meeting Server/ Management, TelePresence Management Server)

Messaging
(Unified CM IM & Presence)

Edge
(Expressway MRA/B2B, voice gateway/CUBE, web proxy, firewalll/VPN)

CALLING

Calling
(Unified CM, Unity Connection (voicemail))

ENDPOINTS

Endpoints
(Desk phones, video/ room, desktop/mobile client (Jabber))

Enterprise Services
(Identity/Directory, Certificate Authority, Calendaring)

REMOTE ENDPOINTS

CLOUD

Collaboration Deployment: Cloud

ON-PREMISES

Cloud Enterprise Services

(Cloud Directory (Azure, Okta), Calendar (O365, Google), Identity Provider)

Cloud Directory / Identity / Calendar

Public CA

CLOUD ENTERPRISE SERVICES

Edge

(Webex Video Mesh (VMN), web proxy, firewall, identity provider (IdP))

EDGE

IdP

INTERNET

REMOTE ENDPOINTS

Webex Control Hub

PSTN

webex

Admin

ENDPOINTS

Endpoints

(Desk phones, video/room, desktop/mobile client (Webex App))

MEETINGS

MESSAGING

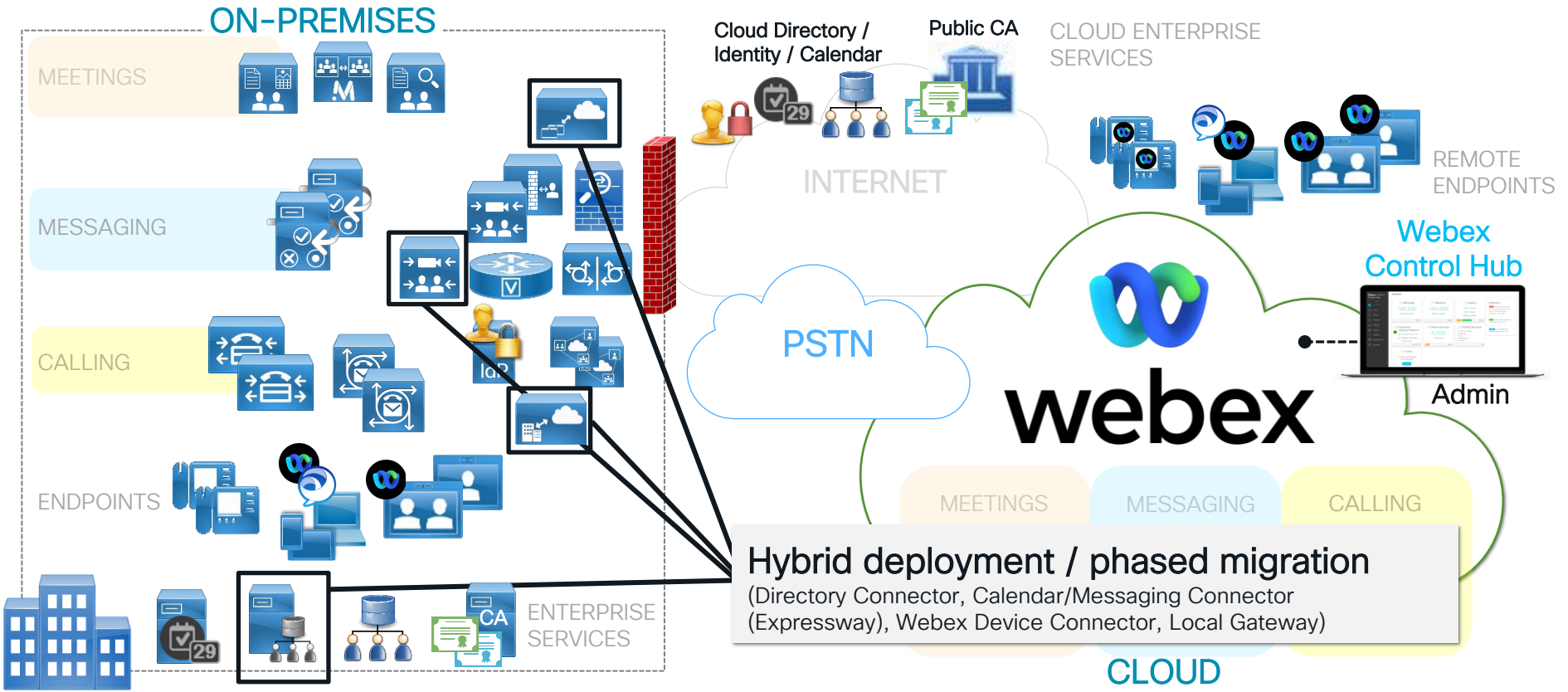
CALLING

Meetings, Messaging, Calling

(Webex)

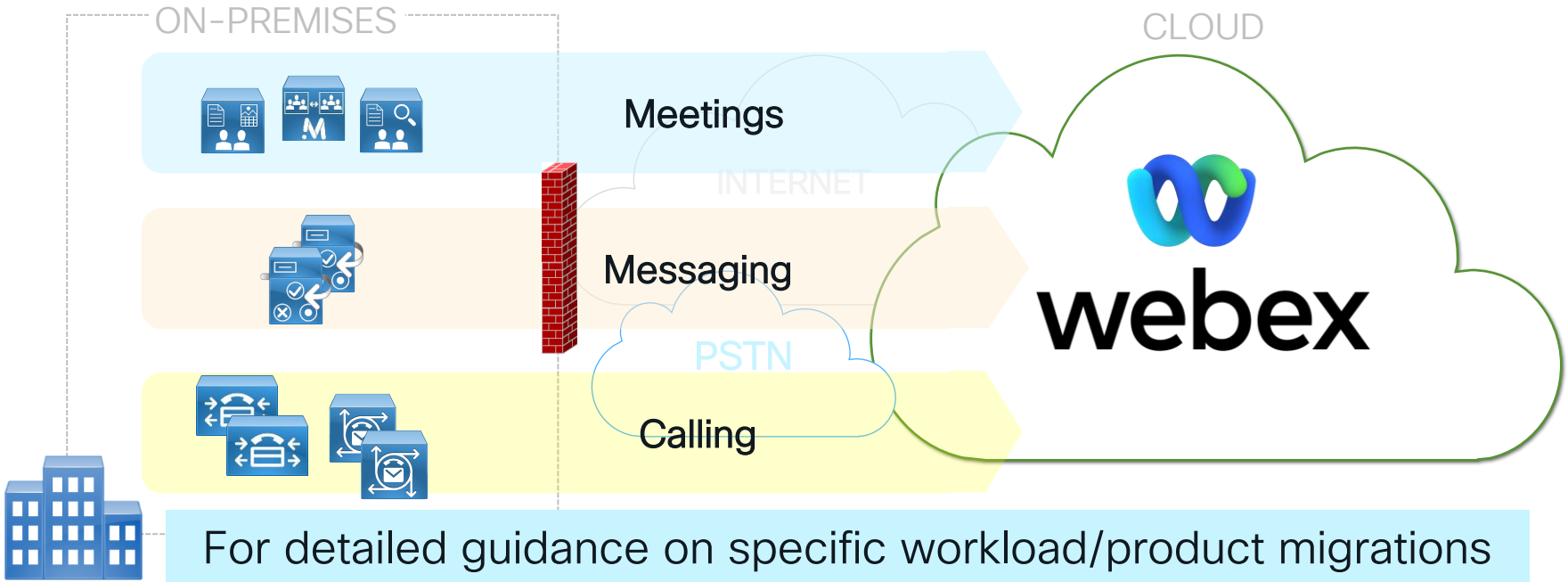
CLOUD

Collaboration Deployment: Hybrid/Phased



Hybrid deployment / phased migration
(Directory Connector, Calendar/Messaging Connector (Expressway), Webex Device Connector, Local Gateway)

Migration by Workload



For detailed guidance on specific workload/product migrations refer to the ***Collaboration Transitions*** transition maps and deployment guides available at https://www.cisco.com/go/ct

Migration Steps Vary by Workload

FOR YOUR REFERENCE

Meetings Update Journey

webex

Migration Ready

webex

Pre-Migration

Create Webex org

- Create / Verify Production Webex Org
- Add / Verify Licenses

Control Hub Setup

- Link SA Webex Sites & Users
- *Verify / Claim Domain(s)*
- *Auto License Templates*
- *Claim Users*
- *Deploy SSO*
- User Provisioning *(Directory Connector, SCIM, CCUC, CSV, Manual, API)*
- *Deploy Hybrid Calendar*

Network / Security Readiness

- Validate Network Connectivity
- Security / InfoSec Approvals

Application Readiness

- Verify / Update Webex Meeting site version
- Verify / Update WDA version

Migration Prep

Control Hub Config

- Verify users are assigned correct meeting licenses
- Verify / Enable Org for Full Feature Meeting Experience
- Set Meeting Data Retention Policy
- Review / Configure App update schedule

Application Prep

- Identify client requirements (Desktop, Mobile, VDI)
- Understand deployment options (desktop & mobile)
- Develop migration plan
- Stage Webex App installation file

Rollout & Decom

Application rollout

- End user comms / training
- Update user's app (WDA to Webex App)
- MS Office integration

Complete Migration

- Remove WDA from user's devices

Source: *Jabber to Webex App Migration – Customer Journeys & Readiness* guide available at https://www.cisco.com/go/ct

Migration Steps Vary by Workload

FOR YOUR REFERENCE

Messaging Migration Journey

Migration Ready

Unified CM+ IM&P

webex

Pre-Migration

Create Webex org
- Create / Verify Production Webex Org
- Add / Verify Licenses

Enable Analytics
- *Cloud-Connected UC*
- *Jabber Telemetry*

Control Hub Setup
- *Verify / Claim Domain(s)*
- *Auto License Templates*
- *Claim Users*
- *Deploy SSO*
- User Provisioning *(Directory Connector, SCIM, CCUC, CSV, Manual, API)*

Network / Security Readiness
- Validate Network Connectivity
- Security / InfoSec Approvals

Messaging Interop
- Deploy Hybrid Messaging
- XMPP & SIP Federation

Migration Prep

Control Hub Config
- Configure Control Hub Messaging Features & Services
  - Message retention
  - Content Management
  - External Messaging restrictions
- Review / Configure App update schedule

Application Prep
- Review Protocol Hander integrations
- Identify client requirements (Desktop, Mobile, VDI)
- Understand deployment options (desktop & mobile)
- Develop migration plan
- Stage Webex App installation file

Rollout & Decom

Application rollout
- End user comms / training
- Migrate users (Jabber to Webex App)
- Migrate Jabber Contacts
- MS Office integration
- Update protocol handlers for 3rd party integrations

Complete Migration
- Remove Jabber from user's devices
- Archive persistent chat history
- Decommission IM&P Servers

Source: *Jabber to Webex App Migration – Customer Journeys & Readiness* guide available at https://www.cisco.com/go/ct

Migration Steps Vary by Workload

FOR YOUR REFERENCE

Unified CM Calling Migration Journey

Migration Ready

Unified CM

Unified CM

Pre-Migration

Webex Org
- Create / Verify Production Webex Org
- Add / Verify Licenses

Enable Analytics
- *Cloud-Connected UC*
- *Jabber Telemetry*

Control Hub Setup
- *Verify / Claim Domain(s)*
- *Auto-License Templates*
- *Claim Users*
- *Deploy SSO*
- ***User Provisioning*** *(Directory Connector, SCIM, CCUC, CSV, Manual, API)*
- **Configure Users' Phone Numbers**

Network / Security Readiness
- Validate Network Connectivity
- Security / InfoSec Approvals
- Verify/ Update Internal / External Voice Domains
- Validate DNS SRV Records

UC Applications
- Verify/ Add Licenses
- Software Versions (CUCM, Expwy, CUC)
- Authentication Method (CUCM / CUC)
- *SSO OAuth w/ Refresh Token Flow Config (CUCM, Expwy, CUC)*
- MRA Deployment

Migration Prep

Control Hub Config
- Configure Control Hub Calling Features & Services (UC Profiles, Org settings, Calling settings, Client settings, etc.)
- Review / Configure App update schedule

Unified CM, Expressway Configs
- Verify CUCM / Expwy Configs (End Users configs, ILS, Home clusters, Service profiles, Jabber-config, Security profiles, Secure calls/ SIP OAuth, QoS, Push notifications, etc.)

Application Prep
- Review Protocol Hander integrations
- Identify client requirements (Desktop, Mobile, VDI)
- Understand deployment options (desktop & mobile)
- Develop migration plan
- Stage Webex App installation file

Rollout & Decom

Application rollout
- End user comms / training
- Migrate users (Jabber to Webex App)
- Migrate Jabber Contacts
- MS Office integration
- Update Protocol Handlers for 3rd party integrations

Complete Migration
- Remove Jabber from user's devices

Source: *Jabber to Webex App Migration – Customer Journeys & Readiness* guide available at https://www.cisco.com/go/ct

Migration Steps Vary by Workload

FOR YOUR REFERENCE

Unified CM to Webex Calling Migration Journey

Migration Ready

Unified CM → webex

Pre-Migration

- **Create Webex org**
  - Create / Verify Production Webex Org
  - Add / Verify Licenses
- **Enable Analytics**
  - *Cloud-Connected UC*
  - *Jabber Telemetry*
- **Control Hub Setup**
  - *Verify / Claim Domain(s)*
  - *Auto-License Templates*
  - *Claim Users*
  - *Deploy SSO*
  - *User Provisioning (Directory Connector, SCIM, CCUC, CSV, Manual, API)*
  - Configure Users' Phone Numbers
- **Network / Security Readiness**
  - Validate Network Connectivity
  - Security / InfoSec Approvals

Migration Prep

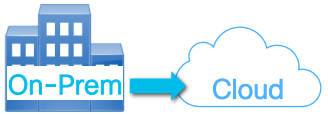
- **Discovery, Planning & Design**
  - Understand UX changes
  - Identify Calling Location, Features & Service requirements
  - Design dial-plan & PSTN/UCM/ PBX Integrations
  - Define 3rd Party, Protocol handler & API integration requirements
  - *UCM Data extraction*
  - *User & Device validation*
- **Control Hub Config**
  - Calling Features & Services (Org settings, Calling settings, Calling features, Dial plan, Client settings, etc.)
  - Locations & Locations services/features
  - Users and Devices
  - Phone numbers
  - PSTN services
  - Deploy UCM/PBX interop - LGW
  - Review / Configure App update schedule
- **Application Prep**
  - Configure 3rd party & API integrations
  - Identify client requirements (Desktop, Mobile, VDI)
  - Understand deployment options (desktop & mobile)
  - Develop migration plan
  - Stage Webex App installation file

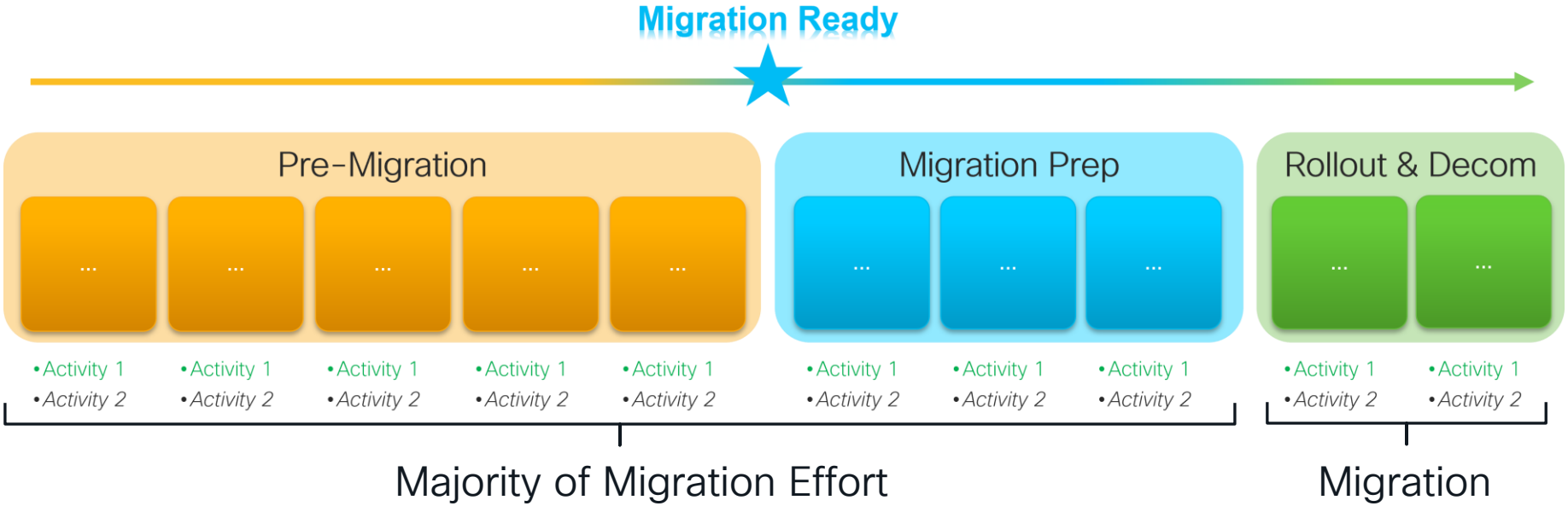
Rollout & Decom

- **Application rollout**
  - End user comms / training
  - Migrate users (UCM to WxC)
  - Migrate Jabber Contacts
  - Migration IP phone FW (Ent to MPP)
  - MS Office integration
  - Update Protocol Handlers for 3rd party integrations
- **Complete Migration**
  - Remove Jabber from user's devices

Source: *Jabber to Webex App Migration - Customer Journeys & Readiness* guide available at https://www.cisco.com/go/ct

Migration: 3 Phase Approach





Security considerations for the migration should be addressed here.

Cloud Migration Best Practices – Security

ON-PREMISES

Meetings

Messaging

Calling

1 **Assess security** of existing on-premises collaboration deployment and **create security migration plan.**

2 **Prepare to migrate existing security** implementations and configuration to the cloud.

CLOUD

3 **Plan for increased security** with additional cloud configuration and integrations.

webex

4 Monitor migration progress and **regularly validate security functionality throughout the migration.**

Privacy and Data Residency

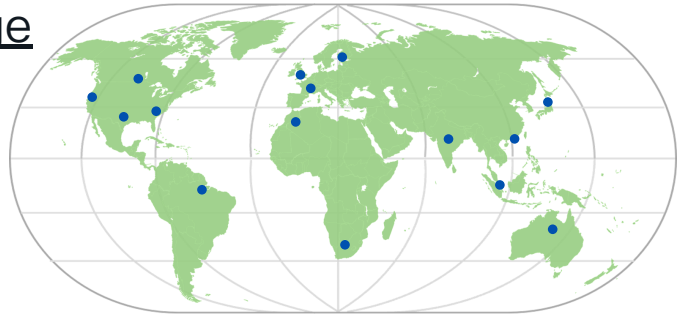
Privacy and Data Residency

Privacy is a critical aspect of collaboration security and relates to the handling of personally identifiable information (PII) and private organizational information.

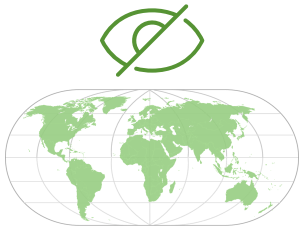
- **What** personal and organizational information is retained?
- **Why** is this information retained?
- **How long** is it retained?

Data residency refers to the protection and storage location of personal and organizational data.

- **Where** is personal and organizational data used, stored, or transferred?
- **How** is this data protected?



Privacy & Data Residency: On-Prem v. Cloud



On-Premises Collaboration

- Personal and organizational data stored in **customer premises data centers.**
- For distributed multi-DC deployments, **data transfers** over secure private network (e.g., MPLS).
- **Data retention** controlled by organization's app/service admin. (e.g., retention period for CDRs, logs, PII, etc.)
- Data optionally **encrypted in transit and at rest.**

Cloud Collaboration

- Personal and organizational data stored in globally distributed **Webex data centers.**
- For organizations with global deployments, **data transfers** over encrypted private backbone.
- **Data retention** controlled by organization admin(s) – with limits.
- Data always **encrypted in transit and at rest.**

Privacy Data Sheets

https://trustportal.cisco.com

Avoid delays during migration rollout

Security and compliance teams within the organization should review appropriate Webex product/service privacy data sheets to understand *how Cisco/Webex handles and protects personal and organizational data* including:

- Types and purpose of personal data Webex processes
- Details of Webex data center locations and legal mechanisms for data transfer across international boundaries
- Who has access to personal data and why
- Data retention and deletion rules
- Details of third-party service providers
- Incident management (PSIRT)

Privacy Data Sheets

https://trustportal.cisco.com

DID YOU KNOW?

Privacy data sheets have been available for Cisco on-premises collaboration products for years.

Privacy: Meetings / Messaging / Calling Data

FOR YOUR REFERENCE

User generated meeting content (including chat) is not persisted in the cloud (unless the meeting is recorded). Option to store and manage meeting recordings, transcripts and file uploads in the Webex cloud.

User generated messaging content is persisted in the Webex cloud.
(messages, files)

User generated calling content is persisted in the Webex cloud.
(voice messages, call recording files)

Detention period configurable by administrator

META DATA

System generated and service-related content for messaging / meetings / calling is persisted in the Webex cloud.
(host / user / usage data for business records, billing, analytics, and troubleshooting)

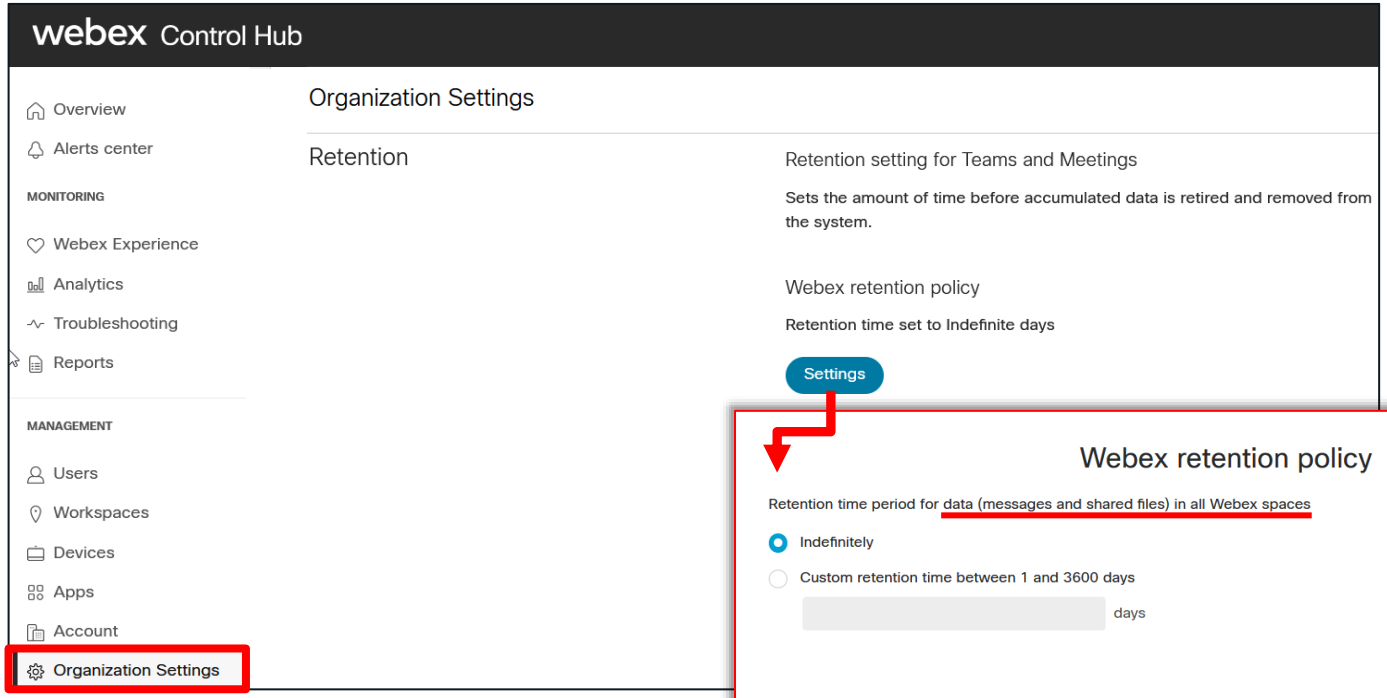
Refer to privacy data sheets

Webex Meetings Privacy Data Sheet | Webex Messaging Privacy Data Sheet | Webex Calling Privacy Data Sheet

Privacy: Messaging Retention

FOR YOUR REFERENCE

Messaging retention policy: Indefinite (default) / Custom (1 – 3600 days)



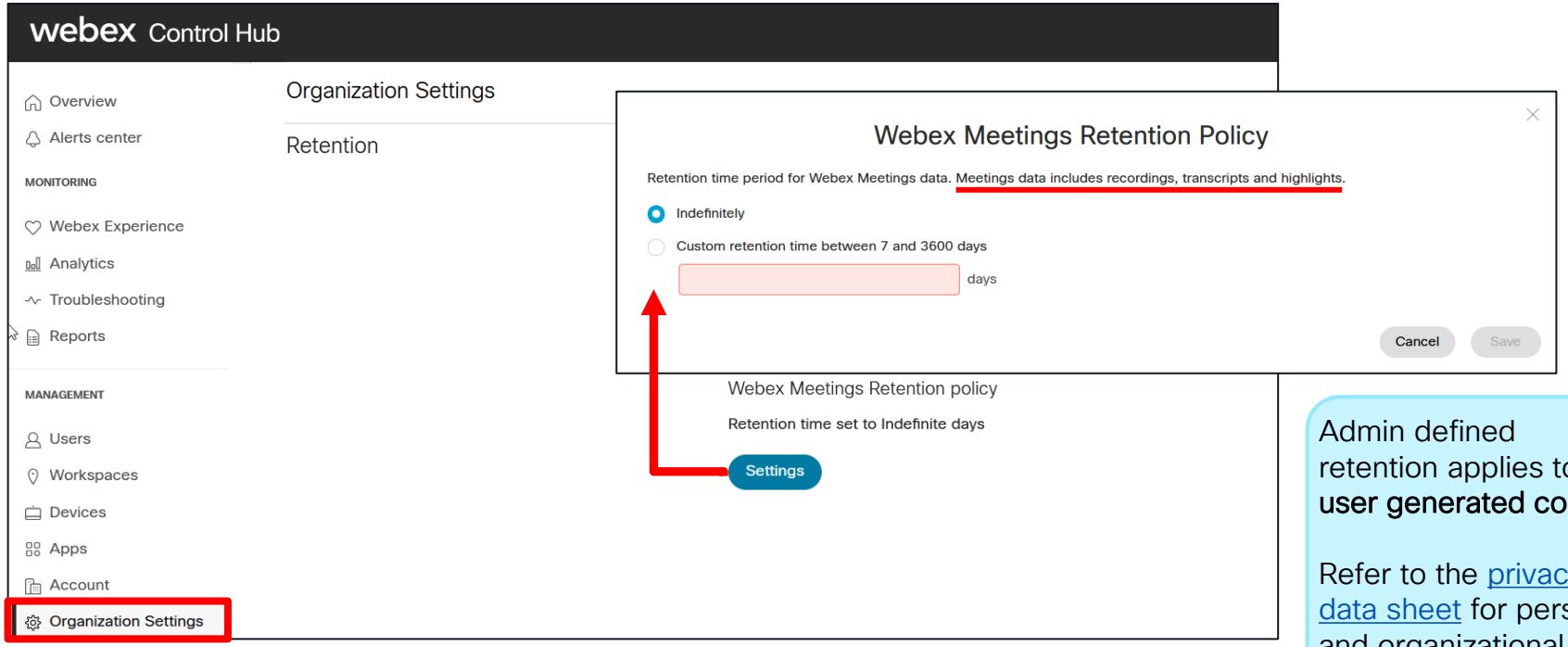
Admin defined retention applies to **user generated content**.

Refer to the privacy data sheet for personal and organizational data retention details.

Privacy: Meeting Retention

FOR YOUR REFERENCE

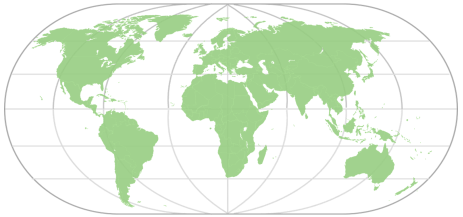
Meeting retention policy: Indefinite (default) / Custom (7 – 3600 days)



Admin defined retention applies to **user generated content**.

Refer to the privacy data sheet for personal and organizational data retention details.

Data Residency

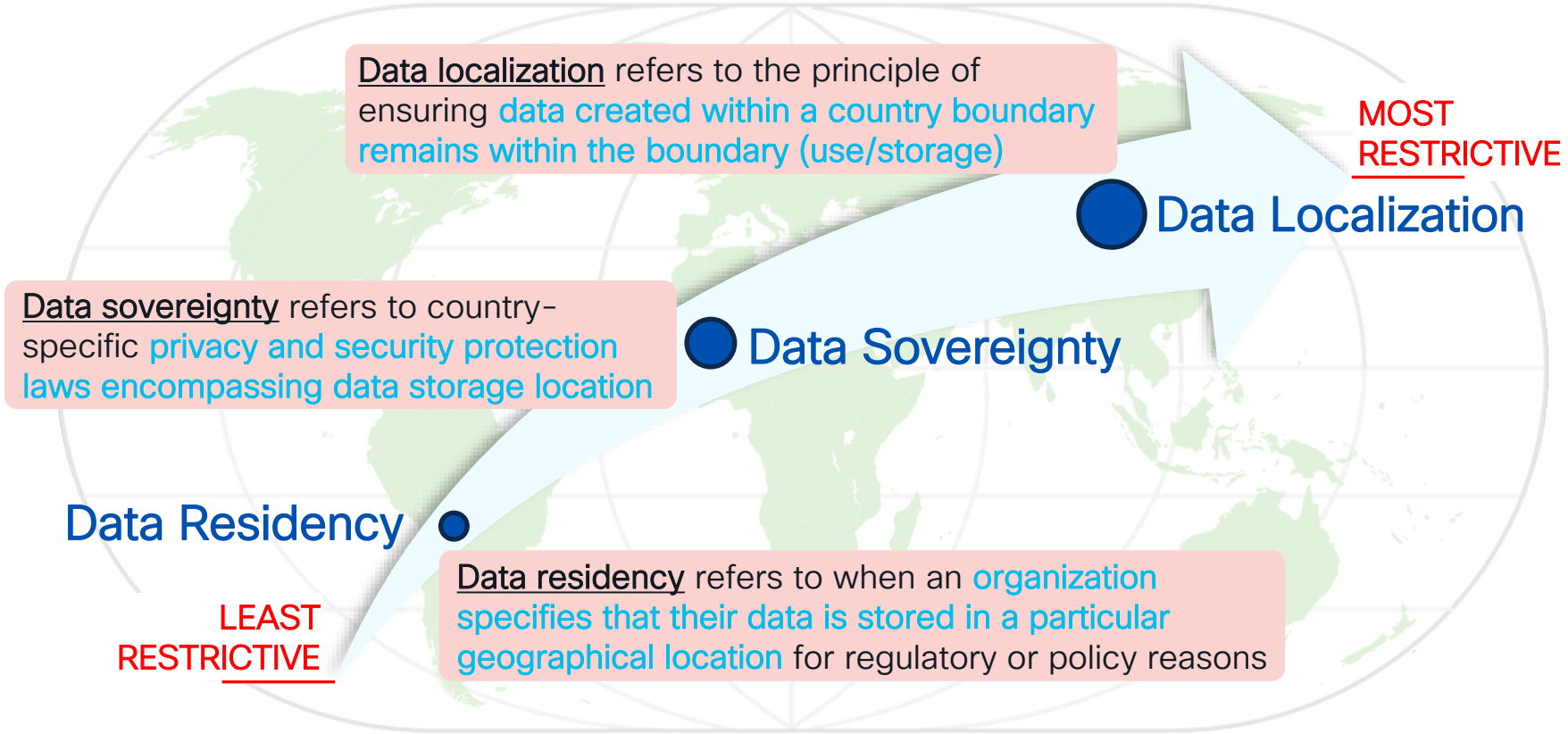


Before proceeding with migration to cloud, ensure regulatory and organizational policy requirements for cloud data residency are understood

- Increasingly, organizations are requiring cloud service vendors to store their **personal and organizational data** in specific geographic locations to meet regulatory and/or policy requirements (legal, taxes, etc.)
- Regulatory requirements vary per region and per country.
- Data stored in the organization's specified location is governed by the privacy and security protection laws of that jurisdiction (data sovereignty)
- Recent Webex DCs have been added to address geographic data residency regulatory requirements: EU (Frankfurt, Amsterdam)

  Canada (Toronto, Montreal)

Data Residency v. Sovereignty v. Localization



FOR YOUR REFERENCE

EU Data Residency Plan for Existing Customers

EU DC – July 2021

- New primary DC. Both Primary/backup DCs in EU
- Operates Meetings, Users, Messaging, Analytics and Calling

UK->EU – Dec 2021

- Migrate User Profiles from London to EU
- Migrated all meeting sites, recordings, transcripts, files

User Profiles & Analytics US -> EU – May 2022

- Customers have option to migrate user profiles (Identity) from US to EU
- Analytics data gets migrated along with User profiles.

Billing and Operational Data – July 2022

- PII transfer to US for billing and administration is stopped for all customers.
- All Webex Orgs created since July 2021 have full data residency.

Org and Messages US -> EU – Q4CY2022

- Customer has option to migrate their Webex organization & messages.
- Once migration is finished, the org has full data residency
- Early customer trials start Q3CY22

Note:

1. User profiles, Org and Messages migration are optional steps that customers will need to schedule once the functionality is available.
2. More details on the migration functionality will be available as we get closer to the release.

Identity and Auth(entication/orization)

Identity and Auth(entication/orization)

Identity relates to users and their privileges.

- What is the source of user information?
- Who has access to resources/services?
- What services are users provisioned for?

Authentication/Authorization refers to the methods by which user identity is verified and service access is granted.

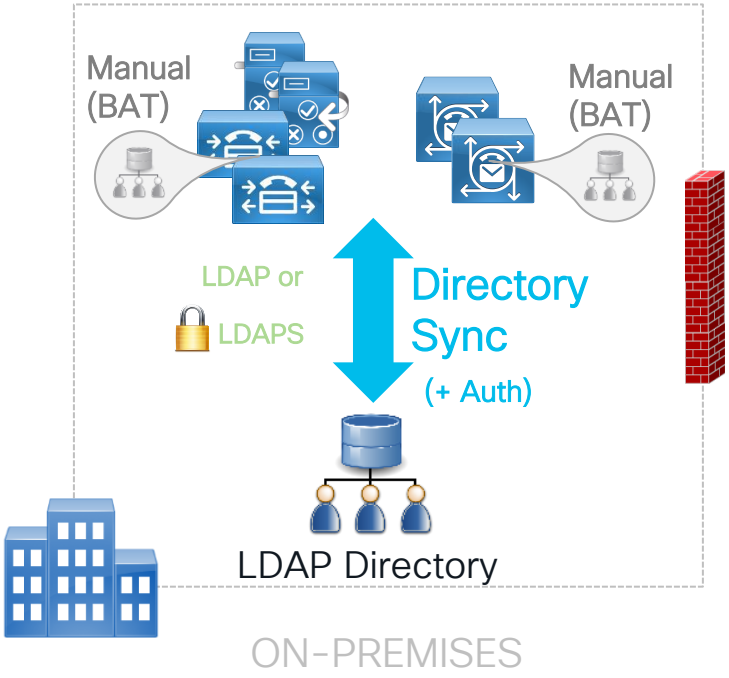
- **How** are users authenticated?
- **How** is access to resources/services protected?

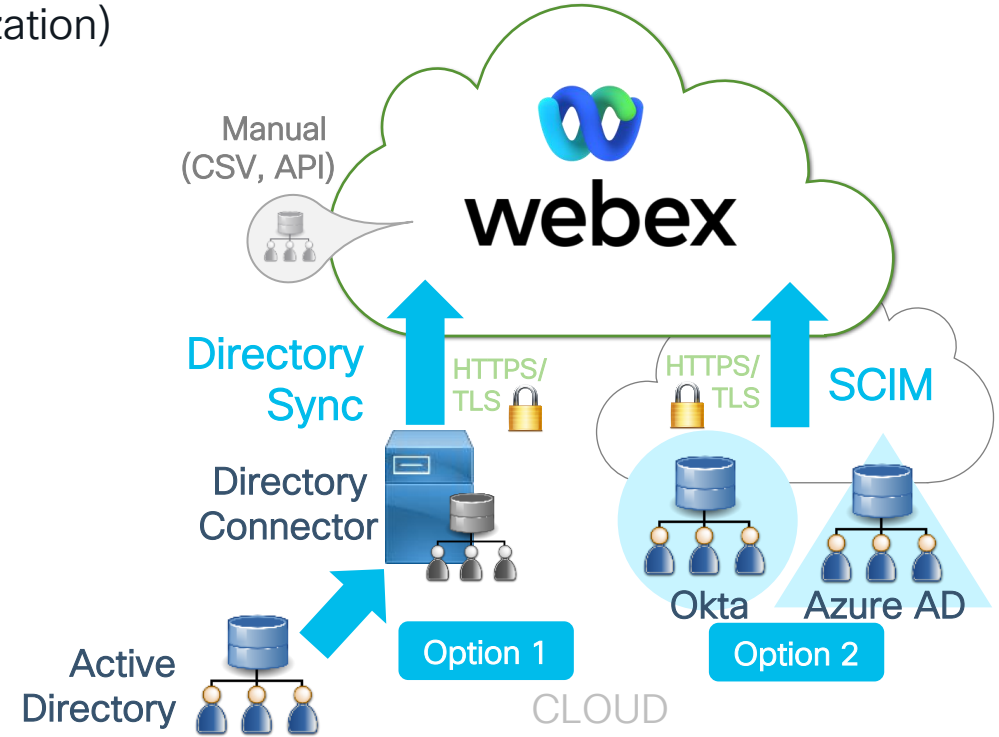
Identity & Auth: On-Prem v. Cloud

On-Premises Collaboration	Cloud Collaboration
User source: Local user database or **LDAP sync** (secure LDAP optional)	User source: Webex cloud identity service (org level) or **directory sync** (e.g., Directory Connector, SCIM).
User provisioning: Manual (BAT for bulk)	User provisioning: Manual (CSV for bulk) or **automated via Directory Connector / SCIM** (e.g., Azure AD Wizard).
User authN/authZ: Local per server/ per service username / password + static access roles. Optionally, **LDAP sync + auth, OAuth** (OAuth access/refresh tokens).	User authN/authZ: Username / password. **OAuth framework**. Optionally, **multi-factor authentication.**
SSO optional (LDAP sync/authentication achieves unified accounts/passwords, no dependency on non-collab IT/security teams).	SSO **highly recommended.**

Identity & Auth: User Identity and Provisioning

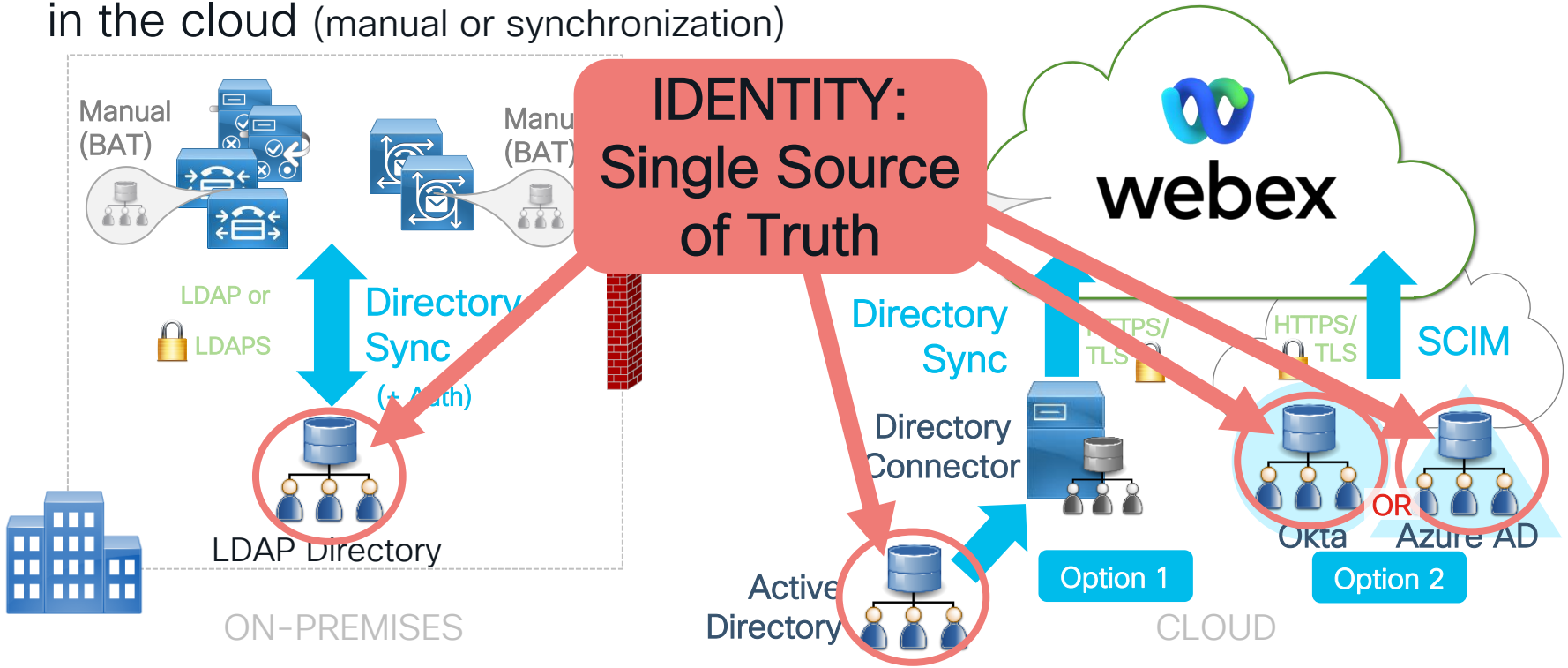
Replicate on-premises user identity & provisioning source in the cloud (manual or synchronization)





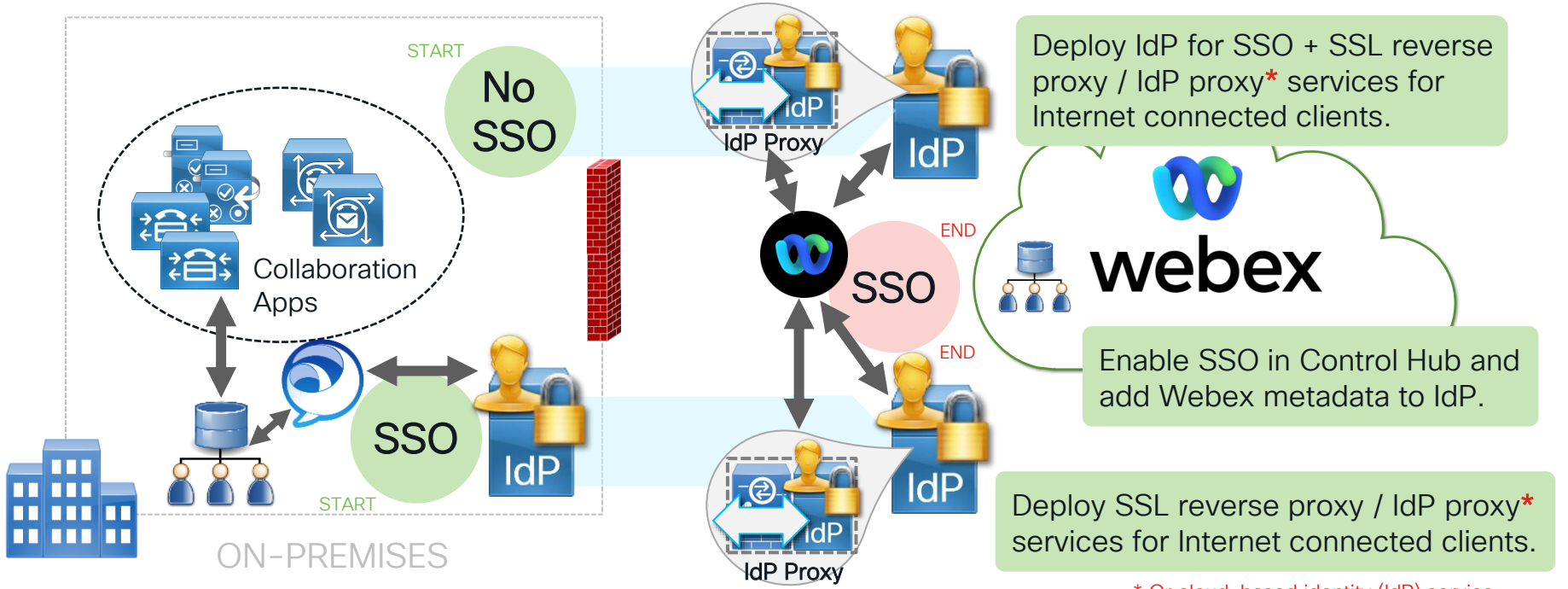
Identity & Auth: User Identity and Provisioning

Replicate on-premises user identity & provisioning source in the cloud (manual or synchronization)



Identity & Auth: Single Sign-On (SSO)

Enable SAML SSO and enroll your Webex org with IdP during migration to ensure seamless operation for users.



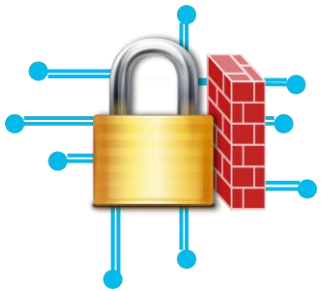
Encryption and Network Considerations

Encryption and Network Considerations

Encryption is a method of securing digital data with a mathematical encoding algorithm to prevent alteration, tampering, and unauthorized access.

- Is data encrypted in transit and at rest?
- Are advanced encryption ciphers available & negotiated?

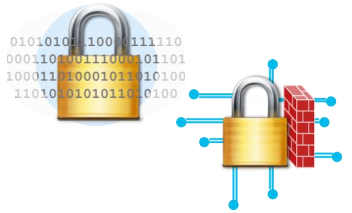
Network security refers to securing data transport and protecting the transport infrastructure* as well as the data it carries from misuse or unauthorized change.



- How do devices and clients connect to services?
- What traffic must be allowed through the firewall/proxy?

* From network edge to data center and extended to include remote users/devices and cloud service access.

Encryption & Network: On-Prem v. Cloud



On-Premises Collaboration

Media/signaling encryption: Optional, but recommended (SIP TLS / SRTP)

Encryption ciphers (on-prem and cloud):

Signaling (TLS 1.2/1.3) → AES_256_GCM_SHA384 or AES_128_CBC_SHA

Media (SRTP) → AEAD_AES_256_GCM or AES_CM_128_HMAC_SHA1

Certificates:

- Server: **Self-signed**, except Expwy-E.
- Endpoints: MIC on devices, LSC optional.
- **Validation by servers/devices, not clients.**

Firewall/proxy: Optional, limited need (no FW traversal, or Expressway MRA)

Cloud Collaboration

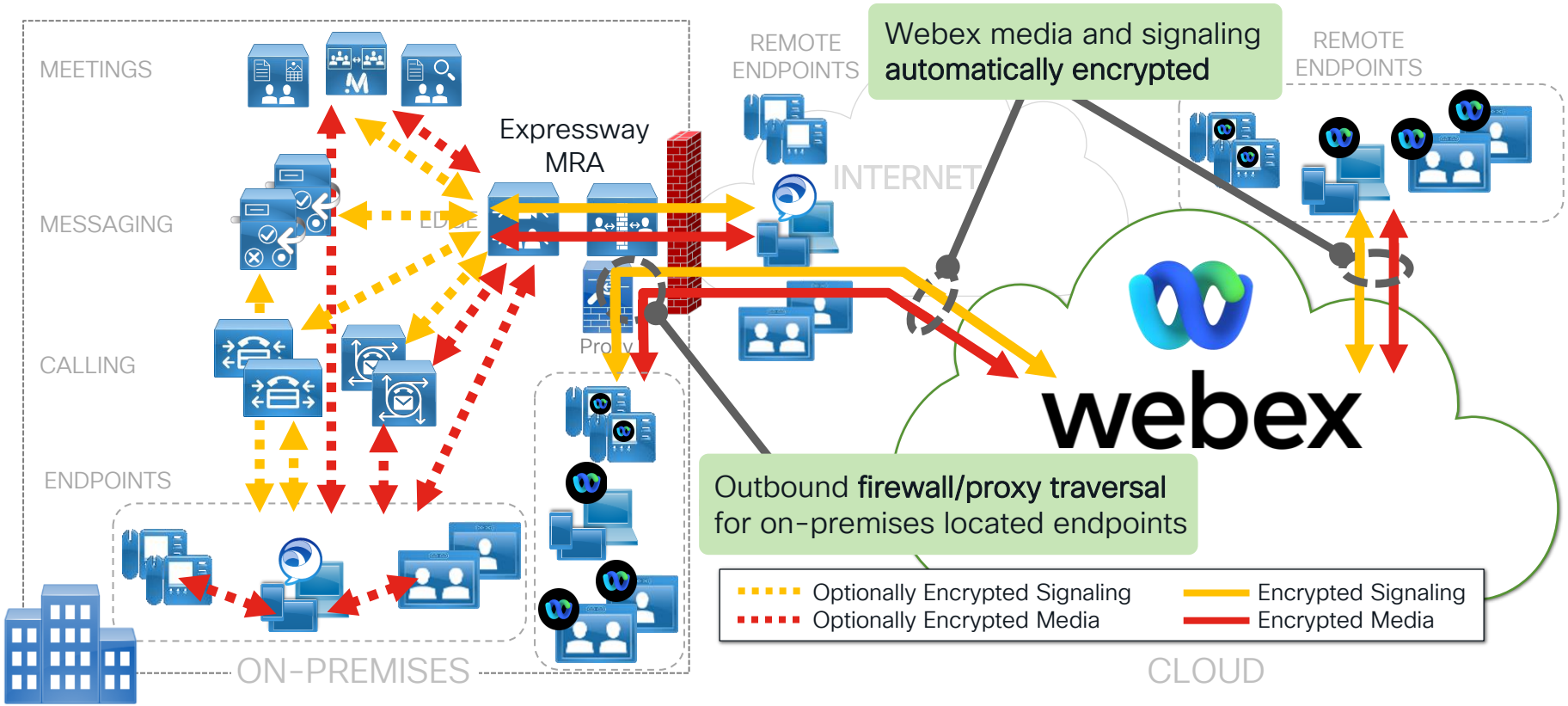
Media/signaling encryption: Mandatory and automatic (HTTPS / SIP TLS / SRTP)

Certificates:

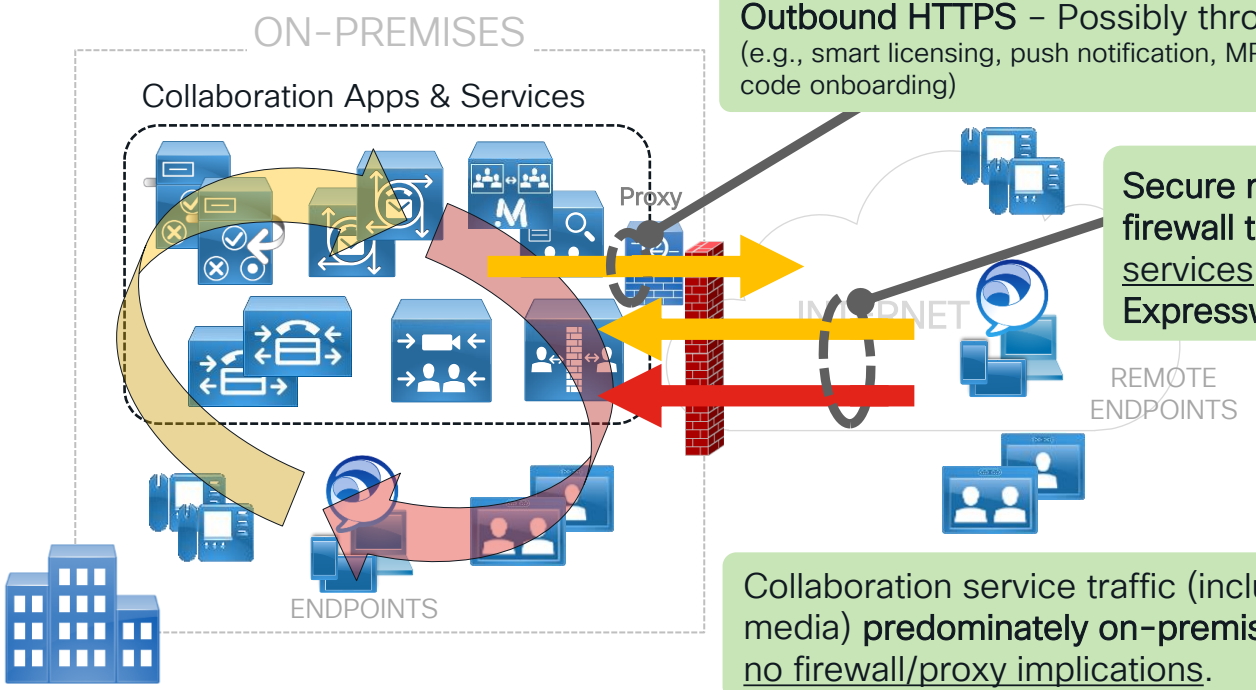
- Cloud services: **Public CA-signed**.
- Endpoints: MIC on devices
- **Validation everywhere**.

Firewall/proxy: Required and extensive – ports, protocols, URLs (signaling) / IP addresses (media)

Encryption & Network: Secure Signaling & Media



Encryption & Network: On-Prem – Firewall/Proxy



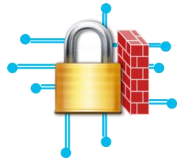
Outbound HTTPS – Possibly through proxy (e.g., smart licensing, push notification, MRA activation code onboarding)

Secure remote endpoint access/ firewall traversal for on-premises services. Signaling/media through **Expressway MRA***

Collaboration service traffic (including media) **predominately on-premises**, no firewall/proxy implications.

* Or VPN

Encryption & Network: Cloud – Firewall/Proxy



TLS signaling:
- ✓ Proxy blocks **domains/URLs** not in configured allow list
- ✓ Firewall: **Allow** traffic from **Proxy IP** to **any IP** on **TLS port 443**

Media:
- ✓ Does not traverse proxy
- ✓ Firewall: **Allow** outbound traffic from **any IP*** to **any IP** (or **Webex media IP addresses**)

ON-PREMISES

ENDPOINTS

Proxy

SIGNALING

MEDIA

Signaling: TLS 443

Media: UDP 5004
TCP 5004
TLS 443

webex

SIGNALING

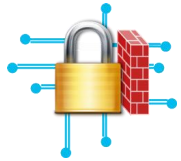
MEDIA

REMOTE ENDPOINTS

Collaboration service traffic (including media) **predominately traverses** the firewall and proxy.

* Or endpoint subnets

Encryption & Network: Cloud – Firewall/Proxy



TLS signaling:
- ✓ Proxy blocks **domains/URLs** not in configured allow list
- ✓ Firewall: **Allow** traffic from **Proxy IP** to **any IP** on **TLS port 443**

Media:
- ✓ Does not traverse proxy
- ✓ Firewall: **Allow** outbound traffic from **any IP*** to **any IP** (or **Webex media IP addresses**)

ON-PREMISES

ENDPOINTS

Proxy

SIGNALING

Signaling: TLS 443

MEDIA

Media: UDP 5004

~~TCP 5004~~

~~TLS 443~~

webex

Collaboration service traffic (including media) **predominately traverses** the firewall and proxy.

* Or endpoint s

***** CAUTION *****

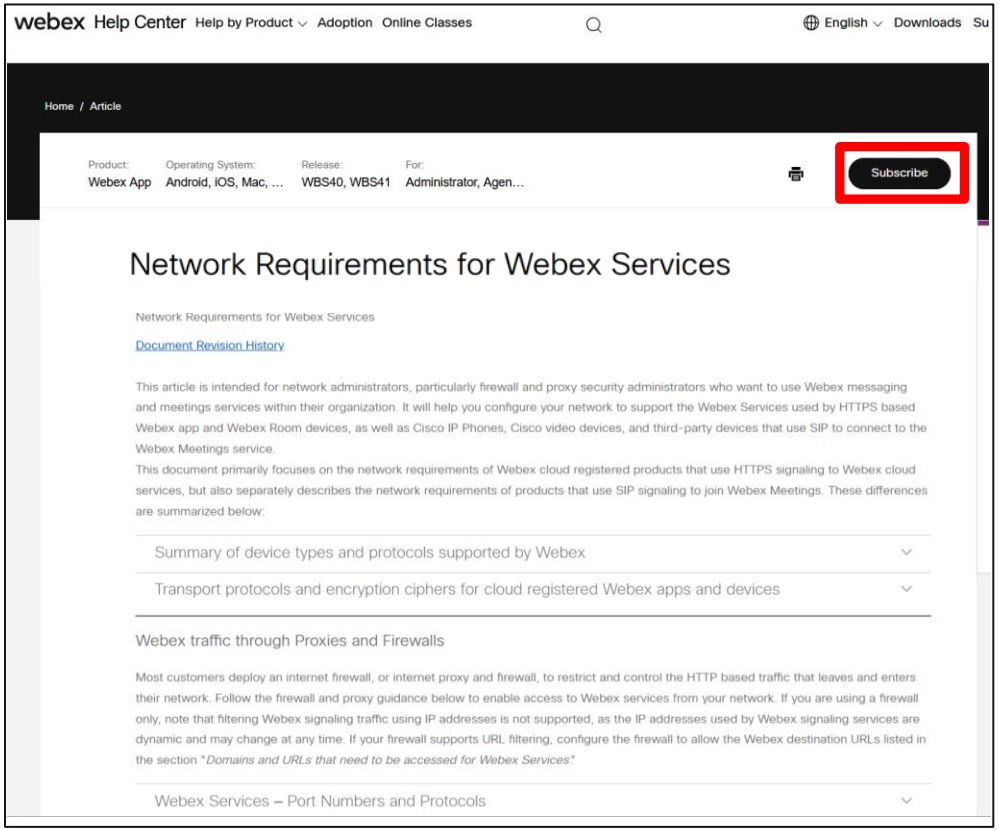
Cisco does not recommend TCP or TLS transport for media. These connection-oriented protocols will result in **poor quality audio & video**.

Encryption & Network: Network Requirements

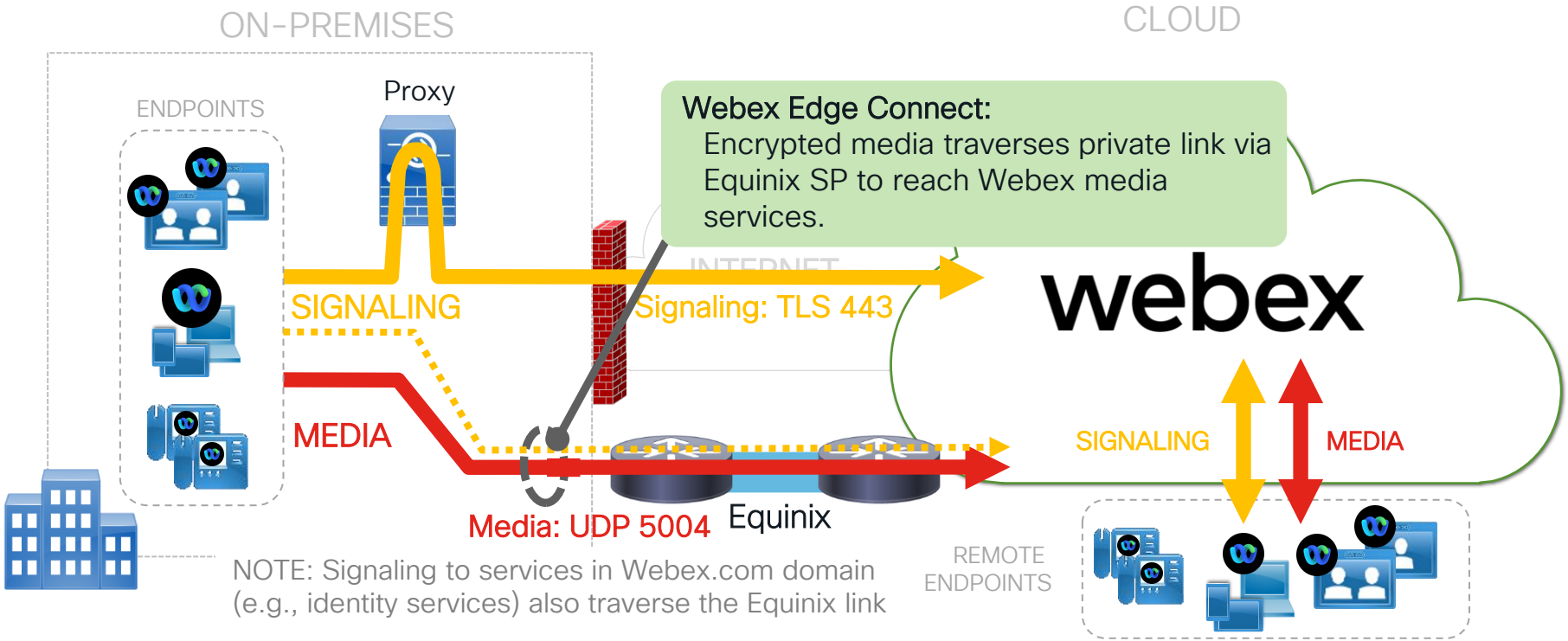
What are the **Webex media IP addresses** that should be allowed through the firewall?

What **domain**s should be allowed through the proxy for proper Webex operations?

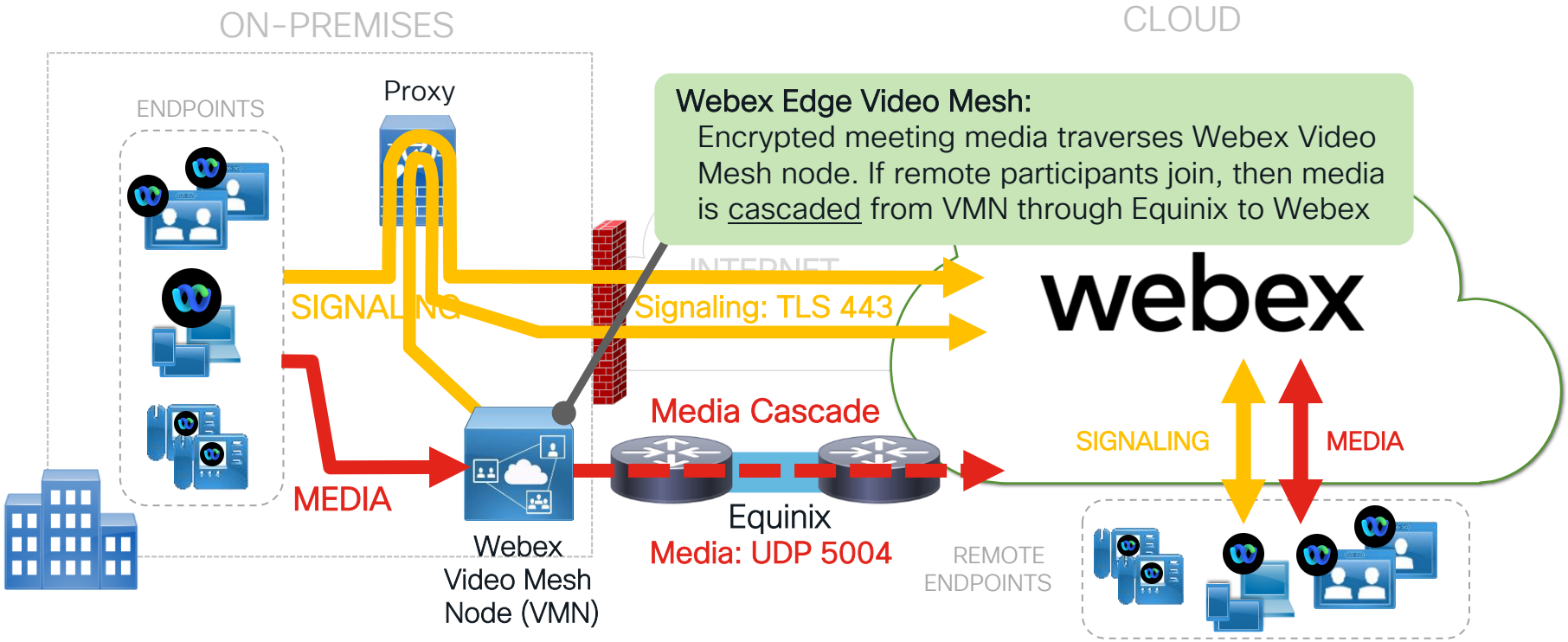
For answers to these questions and for more information about Webex services network requirements, refer to the *Network Requirements for Webex Services* article available at https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services



Encryption & Network: Webex Edge Connect



Encryption & Network: Webex Edge Video Mesh



Compliance and Data Control

Compliance and Data Control

Compliance refers to:

1. **Data control compliance**
   - » Is your data protected from loss or unauthorized access?
2. **Product or service compliance**
   - » How can you trust the products/ services in use adhere to appropriate industry and security standards?

Independent 3rd party audits/ certification

Data control is the ability for an organization to protect its data from unauthorized access and loss. In some cases, data protection is compulsory for organizations due to legal, financial, and/or corporate policies and regulations.

Compliance & Data Control: On-Prem v. Cloud

On-Premises Collaboration

Data control generally optional – org data **typically does not leave org premises.** (Exception: federated messaging)

Data logging/archiving of org and user generated content is optional.*

Data archiving and loss prevention (DLP) integrations with databases and 3rd party products are available.

On-premises **compliance certification /attestation** (FIPS, CC, PCI)

Cloud Collaboration

Data control mandatory – org data **travels outside the premises and resides in the cloud**. Messaging is federated by default.

Data logging/archiving of org and user-generated content is automatic.

Data archiving and loss prevention (DLP) integrations with 3rd party products are **highly recommended**.

Cloud **compliance certification/attestation** (ISO, SOC, CSTAR, C5, FedRAMP, pen tests, etc.)

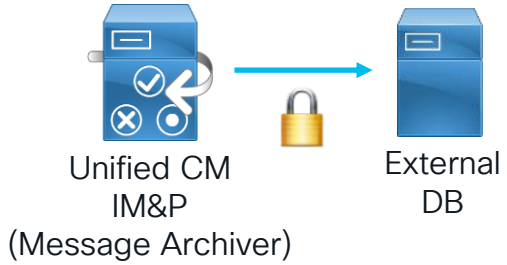
* Unless required by regulation/policy

Data Control: On-Premises Messaging

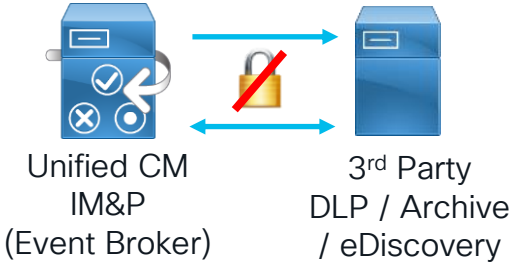
Data Loss Prevention (DLP) allows orgs to control & protect data

Optional on-premises DLP controls available with Jabber and Unified CM:

- Message Archiver – Non-blocking compliance logging (requires external DB – PostgreSQL, Microsoft SQL, or Oracle)



- 3rd party compliance – Blocking compliance and archiving/logging with compliance profiles and profile routing priority.



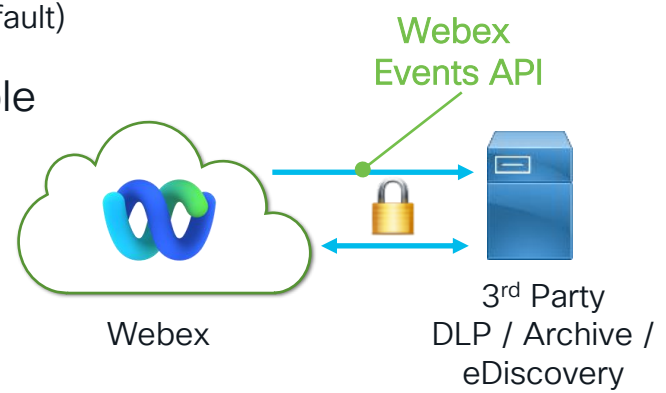
Data Control: Cloud Messaging

Replicate on-prem data controls in the cloud

Even if no on-prem data control compliance is required, data control in the cloud is highly recommended post migration.

Webex supports DLP controls for Webex messaging:

- Automatic, federated **persistent messaging** with indefinite retention in the cloud.
- Granular configuration for **controlling or blocking**: file sharing, external communication, anti-malware (all allowed by default)
- Native *eDiscovery Search and Extraction* tool available for **space activities, messages, and files**.
- 3rd party compliance: Integrations via the **Webex Events API** enabling integration with various DLP (blocking compliance), eDiscovery (search & extraction, legal hold), and Archival (logging) products.



Compliance & Data Control: Certifications

Work with organization's Infosec team or compliance office to review compliance certification for cloud service provider(s) prior to migration

- Because organization data will now traverse and reside off-premises in the cloud, ensuring a cloud service provider meets compliance standards and certifications required by the organization is a critical pre-migration step.

- Compliance certifications and standards audit reports/attestations contain detailed information and validation of a vendor's cloud service operations, information security procedures, and data protection methods.

- Compliance certification is based on independent 3rd party audits using industry standard information security frameworks and methodologies. Certification provides assurances that an organization's data is secure.

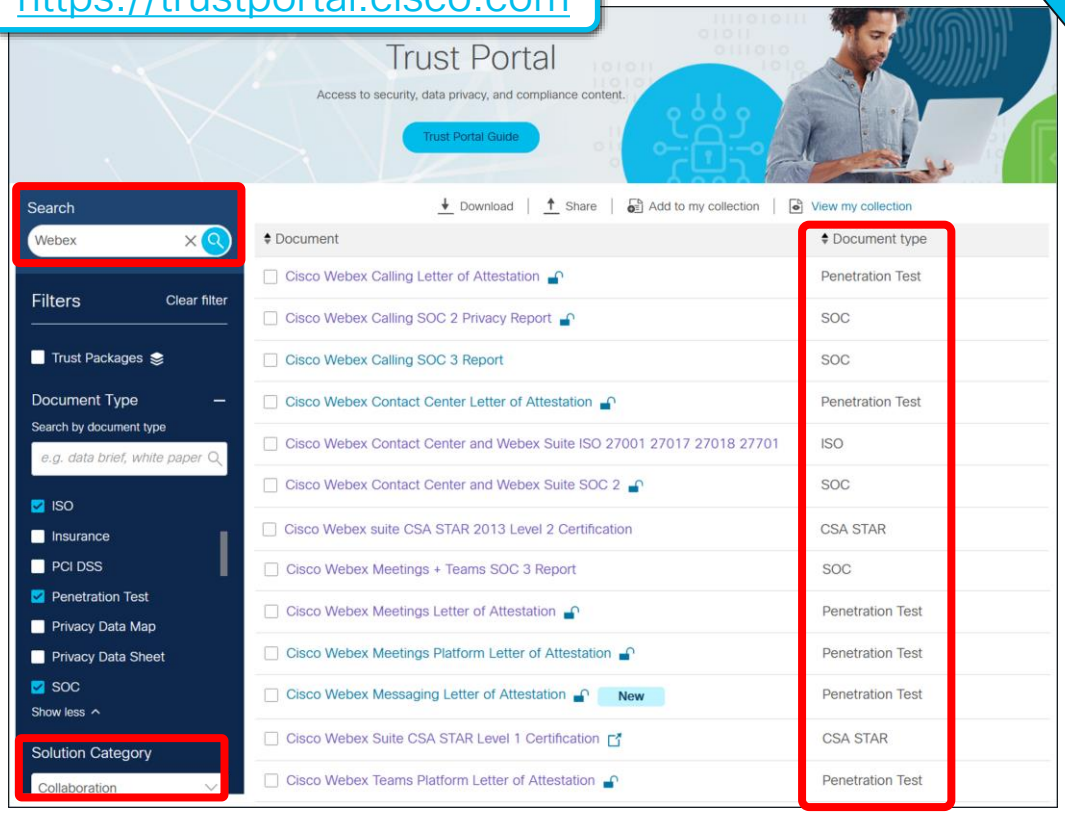
Compliance & Data Control: Certifications

FOR YOUR REFERENCE

Annual standards certifications/ attestations & penetration tests by 3rd party auditors/testers.

- ✓ **ISO 27001- Information Security** (International Organization for Standardization)
- ✓ **SOC 2/3** (System and Organization Control)
- ✓ **CSA STAR** (Cloud Security Alliance - Security, Trust, and Assurance Registry)
- ✓ **C5** (Cloud Computing Compliance Criteria Catalogue)
- ✓ And more...

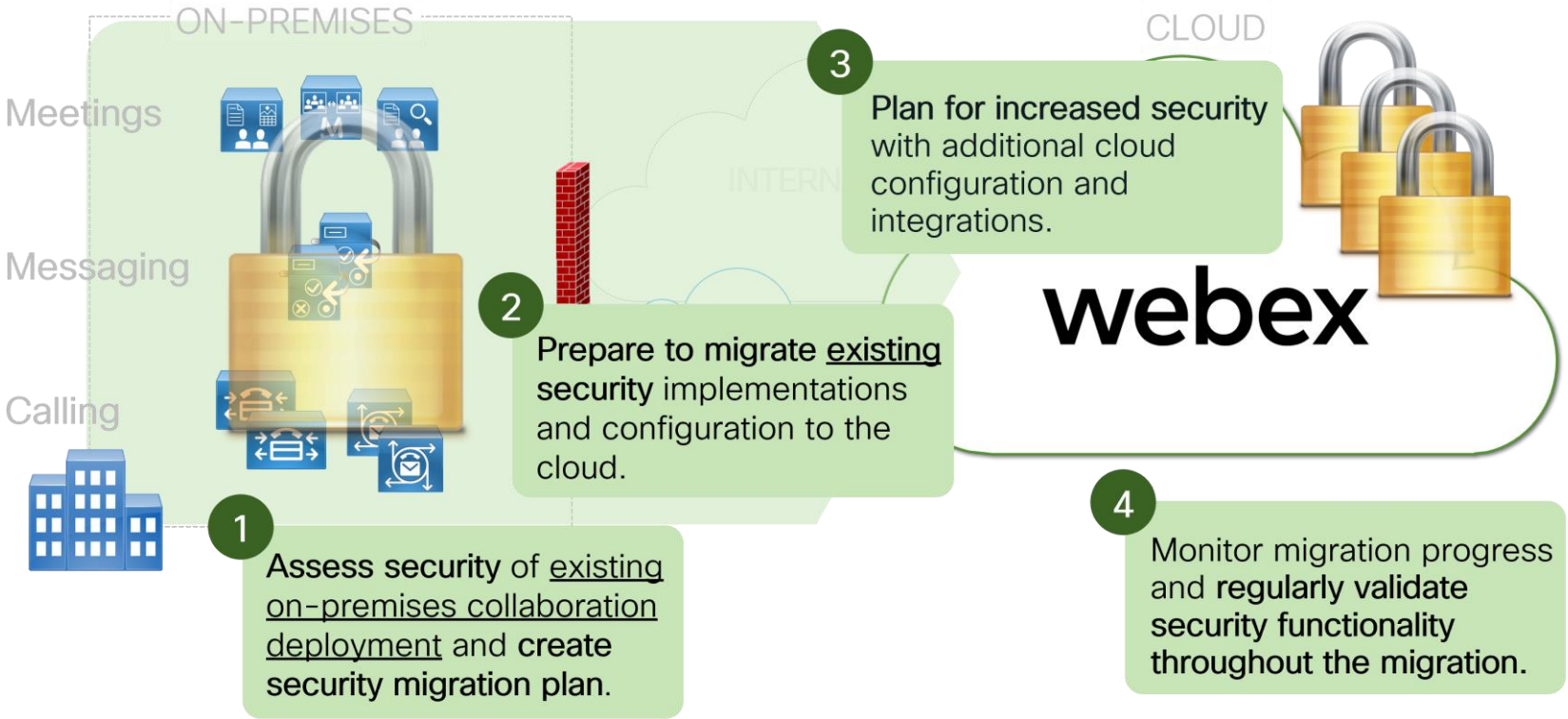
https://trustportal.cisco.com



Conclusion

Collaboration Security

Privacy Identity Encryption Compliance



Key Takeaways

- Cloud deployments are inherently less private and more open; **however,** encryption and data protection capabilities are generally more advanced.
- Understand **how** Cisco secures personal and organizational data in the cloud and **where** your data resides.
- Determine the best option for syncing user identity to Webex and consider deploying single sign-on (SSO).
- Prepare to update firewall and proxy configuration to accommodate Webex services in your deployment.
- **Replicate existing on-premises data control** configuration and integrations to ensure organization data remains protected.

References

- Collaboration Transitions

  https://www.cisco.com/go/ct

- Directory Connector Deployment Guide

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/directoryconnector/cmgt_b_directory-connector-guide-admins.html

- Synchronize Azure Active Directory / Okta users into Control Hub

  https://help.webex.com/en-us/article/6ta3gz/Synchronize-Azure-Active-Directory-users-into-Control-Hub

  https://help.webex.com/en-us/article/nmm9pzdb/Synchronize-Okta-users-into-Control-Hub

- Network Requirement for Webex Services

  https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services

- Port Reference Information for Cisco Webex Calling

  https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

- DLP / eDiscovery / Archive

  https://help.webex.com/en-us/article/nmbm0jk/Webex-App-integration-with-archiving-and-data-loss-prevention-solutions

- Cisco Trust Portal

  https://trustportal.cisco.com/

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Related Sessions This Week (1 of 2)

Collaboration Security:

- **BRKCOL-2007a** Authentication, Authorization & Provision for Cisco Collaboration – Part 1
- **BRKCOL-2007b** Authentication, Authorization & Provision for Cisco Collaboration – Part 2
- **BRKCOL-2057** Understanding Network Security Requirements for Webex Traffic*
- **BRKCOL-2876** Securing Webex Meetings – Privacy, Confidentiality & Security options for meetings in a virtual world

cisco Live!

Related Sessions This Week (2 of 2)

Collaboration Migrations:

- **BRKCOL-2245** Webex Migration Readiness – Calling, Messaging & Meetings*
- **BRKCOL-2029** Journey to Cloud – Webex Edge for Devices
- **BRKCOL-2481a** Successful Migrations from Unified CM to Webex Calling – Part 1
- **BRKCOL-2481b** Successful Migrations from Unified CM to Webex Calling – Part 2

Thank you


cisco Live!
ALL IN