cisco *Live!*

Let's go
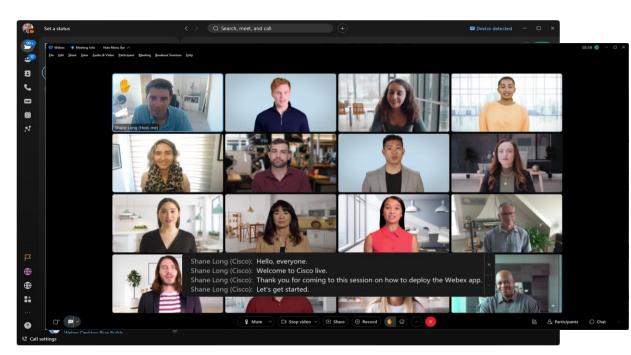
Agenda

- Introduction

- Webex Organization Setup

- Meetings Platform Update

- Webex App Calling

- App Deployment

- Messaging Demo

cisco *Live!*

The Webex App

One easy-to-use and secure app to call, message, meet and get work done.

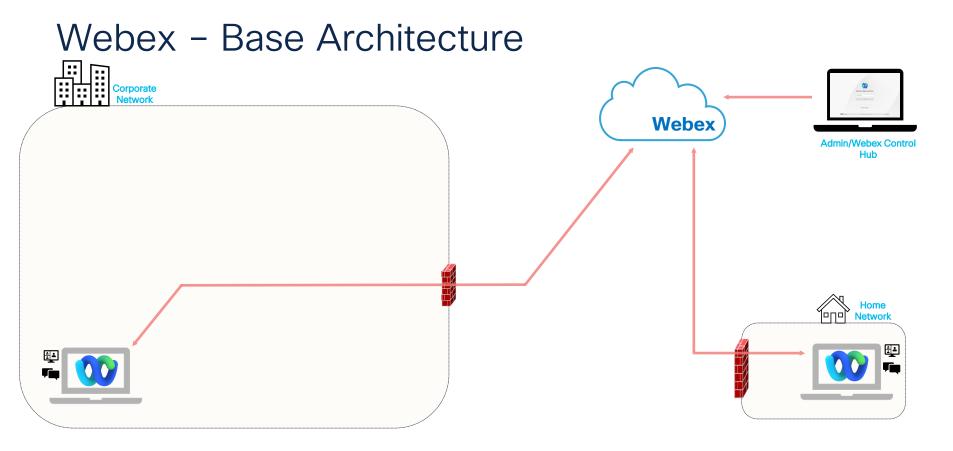### Full Webex meetings experience
Webex meetings platform evolution

Enterprise Grade Calling
Unified CM
Webex Calling
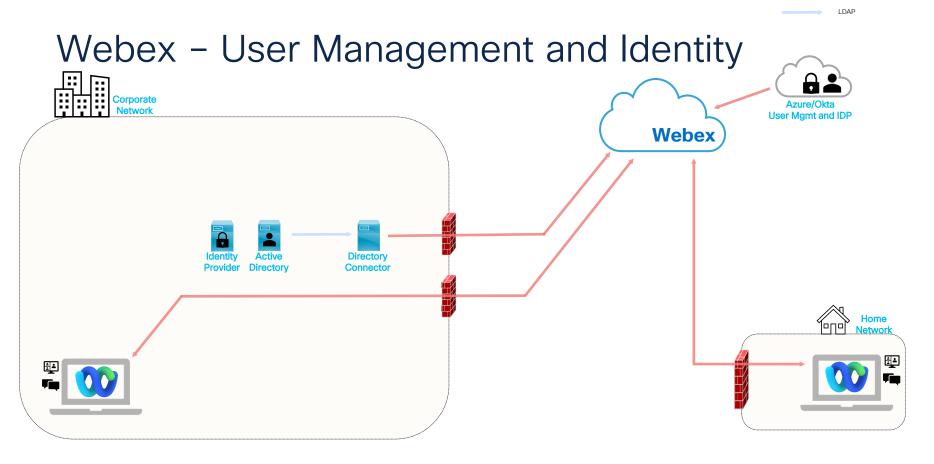
Modern messaging capabilities
Powerful 1:1 and 1:many messaging and sharing capabilities

Customizable app experience
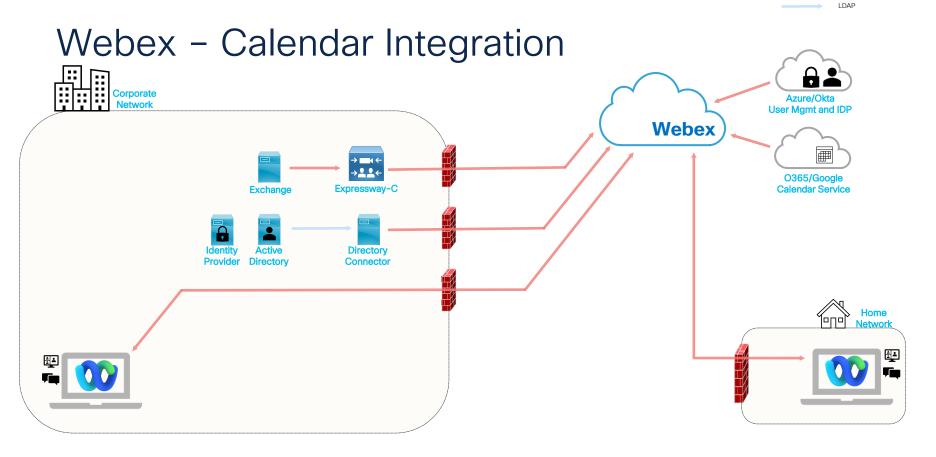Enable the features and services that you need
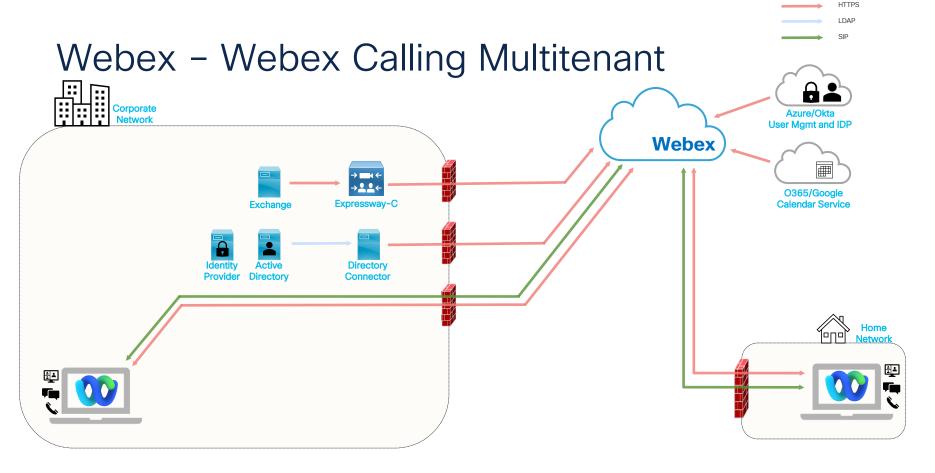
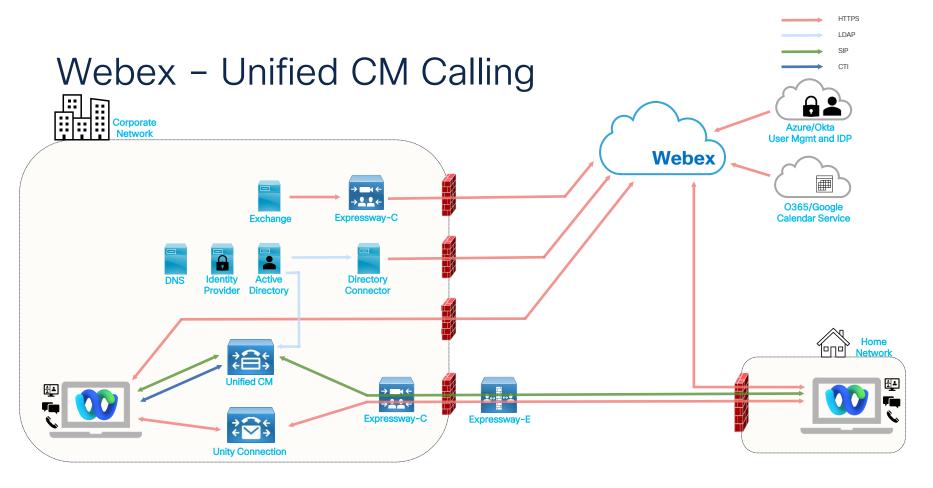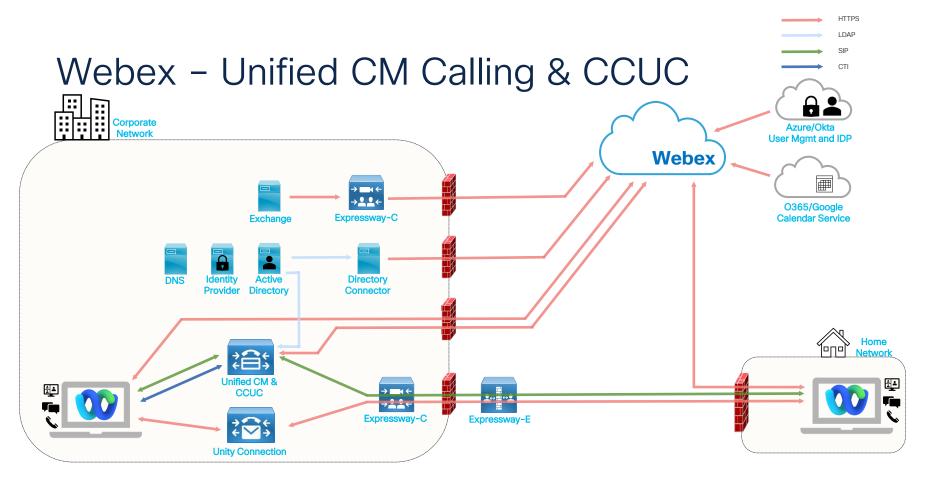# Webex – Base Architecture

Corporate Network

Webex

Admin/Webex Control Hub

Home Network

Webex – User Management and Identity

Webex – Calendar Integration

Webex – Webex Calling Multitenant

Webex – Unified CM Calling

Webex – Unified CM Calling & CCUC

Legend:
- HTTPS
- LDAP
- SIP
- CTI

Corporate Network

Exchange — Expressway-C

DNS — Identity Provider — Active Directory — Directory Connector

Unified CM & CCUC

Unity Connection

Expressway-C — Expressway-E

Webex

Azure/Okta User Mgmt and IDP

O365/Google Calendar Service

Home Network

Webex Org and User Identity

Typical Webex App Deployment

Org Basic Setup	Authentication	User and Group Management	Licensing	Service and App Configuration	App Deploy
✓ Verify Domain ✓ Claim Domain	✓ Enable SSO	✓ User Sync ✓ Claim Users	✓ License Templates	✓ App Experience ✓ Message ✓ Meet ✓ Calling	✓ Desktop ✓ Mobile ✓ Continuous Monitoring

User Authentication

Basic Authentication

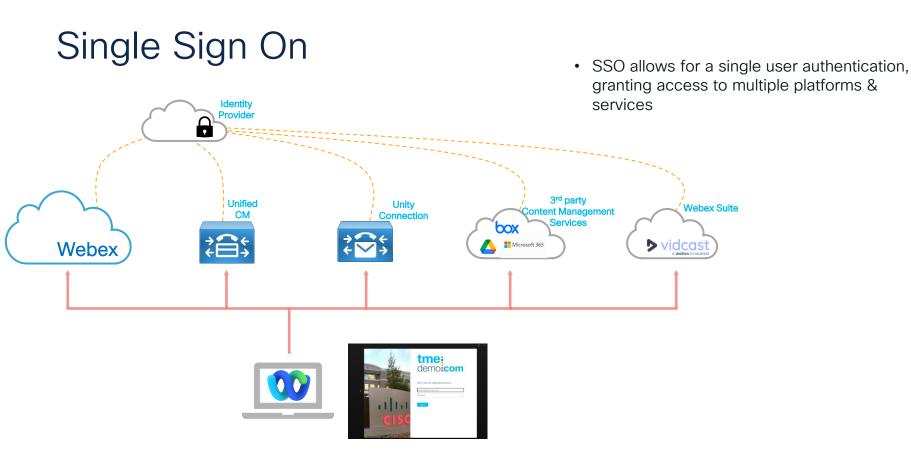- Email & Webex password
- Duo Integration

Single Sign On

- Any auth type supported by the IDP, MFA
- Common user identity across all services/platforms
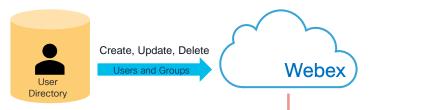- NEW – Support for Multiple IDPs per org (Extended Security Pack Required)

Single Sign On

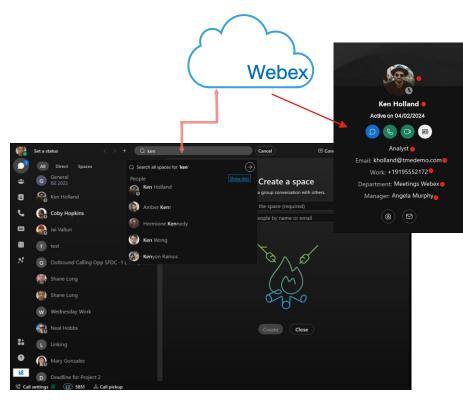- SSO allows for a single user authentication, granting access to multiple platforms & services

Identity Provider

Webex

Unified CM

Unity Connection

3rd party Content Management Services

box

Microsoft 365

Webex Suite

vidcast
a webex innovation

tme demo com

Webex User Provisioning

Create, Update, Delete
Users and Groups

User Directory → Webex

| Webex Attributes	Details
avatar	Image sourced from a resource server or directory binary data
buildingName	
c	
departmentNumber	
displayName	How user name is displayed in Webex
ds-pwp-account-disabled	
employeeNumber	
employeeType	
externalID	Used to specify a users Azure ID
facsimileTelephoneNumber	
givenName	
jabberID	Used for XMPP messaging
l	
locale	
manager	
mobile	
o	
ou	
phoneNumbers;type-work_extension	
physicalDeliveryOfficeName	
postalCode	
preferredLanguage	
sipAddresses;type-enterprise	
sn	
st	
street	
telephoneNumber	Default Work Phone Number
timezone	Appears in People Ingsights profile
title	
uid	Used to sign into Webex, can be *mail* or *UserPrincipalName*
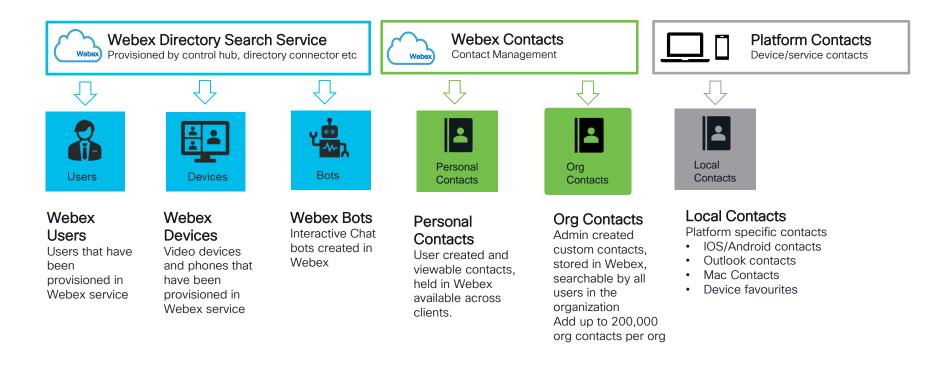
Webex User Search/Resolution

- Webex App will perform directory queries against the Webex Directory Search Service
  - User search
  - User Resolution
  - Phone Number Resolution
  - Avatar Display

- Ensure all necessary user attributes are synced to Webex via user provisioning process

Webex App Contact Search

Webex Directory Search Service
Provisioned by control hub, directory connector etc

Webex Contacts
Contact Management

Platform Contacts
Device/service contacts

Users

Devices

Bots

Personal Contacts

Org Contacts

Local Contacts

Webex Users
Users that have been provisioned in Webex service

Webex Devices
Video devices and phones that have been provisioned in Webex service

Webex Bots
Interactive Chat bots created in Webex

Personal Contacts
User created and viewable contacts, held in Webex available across clients.

Org Contacts
Admin created custom contacts, stored in Webex, searchable by all users in the organization
Add up to 200,000 org contacts per org

Local Contacts
Platform specific contacts
- IOS/Android contacts
- Outlook contacts
- Mac Contacts
- Device favourites

NEW: Hide from Webex App Search

- When enabled, the user and their registered devices cannot be searched from the Webex App

- Example usage:
  "I do not want my CxO to be searchable from the Webex App"

- This does NOT make a user uncontactable – you can still call or message the user if you know their details

Webex User Account Management Solutions

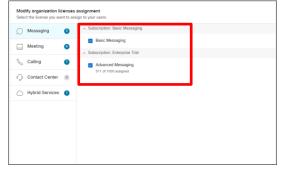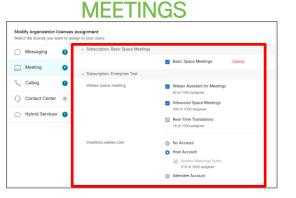| Method	Description
Directory Connector	Automatic method for creating, updating and deactivating user accounts and groups via Active Directory or AD LDS
Microsoft Azure Active Directory Wizard	Automatic method for creating, updating and deactivating user accounts and groups via Microsoft Azure
SCIM	Automatic method for creating, updating and deactivating user accounts via SCIM compliant systems (e.g. Okta)
SAML JIT	Automatic account creation based on SSO login
Self Registration	User can self register to create their Webex account in a claimed org
CUCM User Sync	Create Webex user accounts based on CUCM endusers (via CCUC)
Social Login	Automatic account creation via sign in to third party service for claimed domain (Apple, Google, Facebook, Microsoft)
CSV file	Admin can create and update users by importing a CSV file into Control Hub
API	Admin can create, update delete and list users by using Webex API's
Manual	Admin can use Control Hub to manage user accounts
Meetings Site User Linking	Automatically link Site Admin user accounts to Control Hub

License Template

License Templates allow for configuring of a common licensing model per
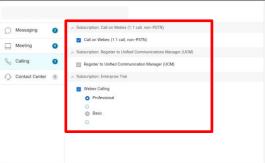
- Organization
- Group
- User

MESSAGING

MEETINGS

CALLING
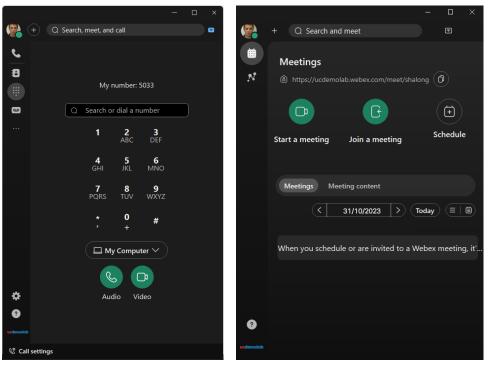
Service Entitlement

Calling Only Mode

Meetings Only Mode

- Services can be selected as needed in the license template

- Permutations of Calling, Messaging and Meetings can be configured

Groups

User Groups can be synced to Webex
- Directory Connector
- Azure AD Wizard
- Groups dev API
- Created Manually in Control Hub
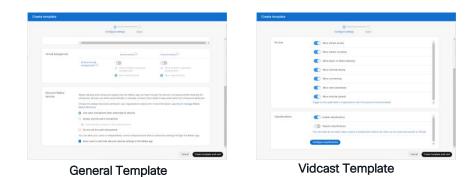
Groups can be used to apply license templates and settings templated to users with common requirements

Settings Templates

General Template

Vidcast Template
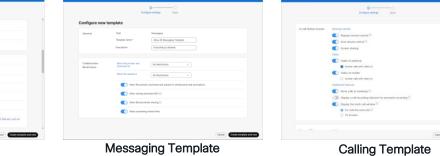
Create a Settings Template to control specific settings for
- General (Organisation Settings)
- Vidcast
- Meetings
- Messaging
- Calling

Meetings Template

Messaging Template

Calling Template

Groups and Settings Templates

The Groups tab allows the admin to assign License Templates and Settings Templates to the User Group

Meetings Platform Update

Webex Meetings Platform Evolution

MC Meeting Platform

Collection of services delivering a meetings platform to a range of endpoint types

Challenges
- Multiple apps on desktop, mobile and VDI (cross launch experience)
- Admins need to track 2 monthly release schedules
- Video Mesh not supported
- No native Linux meetings app
- Space Meetings vs Webex Meetings
- Ephemeral Meetings Chat

Platform Update →

Webex Suite Meetings Platform

A modern meetings platform delivering a consistent experience no matter what device a user joins from
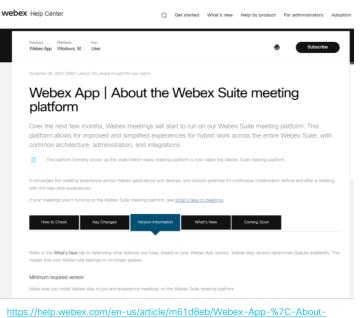
Benefits
- Single app on desktop, mobile and VDI
- Single update schedule for admins to track
- Video Mesh is supported for all Webex Meetings
- Native meetings app on Linux (Webex App)
- Consistent meetings experience when scheduled from a space or a PMR
- Chats & recordings available post meeting to continue collaboration
- Faster join experience
- Increased Video Mesh Capacity
- Join from two devices, appear in the roster once
- AI Ready
- more....

Webex Suite Meetings Platform Readiness

App	Detail
Windows	Webex App
Mac	Webex App
iOS	Webex App
Android	Webex App
VDI	Webex App Webex App VDI plugin
Minimum Version	42.10

Webex Webinar will still run on the MC platform – cross launch experience
Webinar will be updated to the Webex Suite Meetings Platform in CY 2024

Webex Suite Meetings Platform – Key Changes
In-Meeting Chat
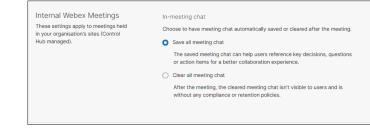
Rich in-meeting messaging is available for meetings hosted on a site enabled for Webex Suite Meetings Platform
- Stored persistently and will be accessible by users from within their Webex App meetings tab
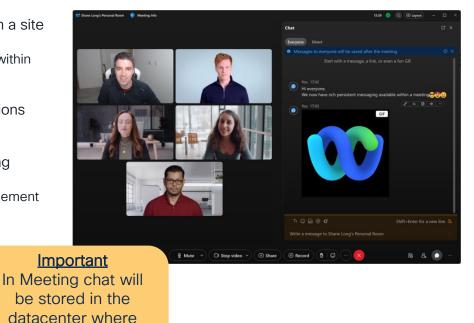
In-meeting messaging content will be subject to the organizations **Meeting Retention Policy**

In-meeting chat enablement is independent Webex ,messaging enablement (via license)
- Control Hub admin can control this In-meeting chat enablement

Internal Webex Meetings
These settings apply to meetings held in your organisation's sites (Control Hub managed).

In-meeting chat
Choose to have meeting chat automatically saved or cleared after the meeting.

○ Save all meeting chat
The saved meeting chat can help users reference key decisions, questions or action items for a better collaboration experience.

○ Clear all meeting chat
After the meeting, the cleared meeting chat isn't visible to users and is without any compliance or retention policies.

Important
In Meeting chat will be stored in the datacenter where your Webex org resides

Webex Suite Meetings Platform – Key Changes
Polling and Q&A

- Polling and Q&A are delivered via Slido for meetings hosted on a Webex Suite Meetings Platform enabled site

- Slido admin and moderation is performed via slido.com

Meeting Center Meeting Firewall Requirements

Meetings signalling and media traffic is Webex App initiated. Outbound firewall rules only need be applied (Firewall should allow return traffic from Webex services)

App Process (Windows)	atmgr.exe
Protocol	UDP
Source Address	Local IP Address
*Source Port Audio	52,000 to 52,049
*Source Port Video	52,100 to 52,199
Destination Address	See Network Requirements for Webex Services for media services IP subnets
Destination Port	9000 (fallback: TLS 443)

*Source ports ranges apply only when dedicated source port settings in place. Otherwise, source ports will be ephemeral

Webex Suite meeting platform Firewall Requirements

Webex Suite meeting platform

Webex

Meetings signalling and media traffic is Webex App initiated. Outbound firewall rules only need be applied (Firewall should allow return traffic from Webex services)

App Process (Windows)	ciscocollabhost.exe
Protocol	UDP
Source Address	Local IP Address
*Source Port Audio	52,000 to 52,049
*Source Port Video	52,100 to 52,199
Destination Address	See Network Requirements for Webex Services for media services IP subnets
Destination Port	5004 (fallback: UDP 9000, TCP 5004, TCP 443)

*Source ports ranges apply only when dedicated source port settings in place. Otherwise, source ports will be ephemeral

Quality of Service

- If a Windows application marks a packet with a DSCP value, Windows will remark the DSCP value to 0

- A Group Policy is required for Windows applications to mark audio, video and screen share with appropriate DSCP markings e.g.
    - Audio DSCP: EF
    - Video and Screen Share DSCP: AF41

- The Group Policy setting typically is configured to mark any packets with a DSCP markings based on:
    - Application Process Path
    - Source/Destination Port

- Action may be required to reimplement a QoS Group Policy, as the in-meeting Windows process is now different, and source port may be different

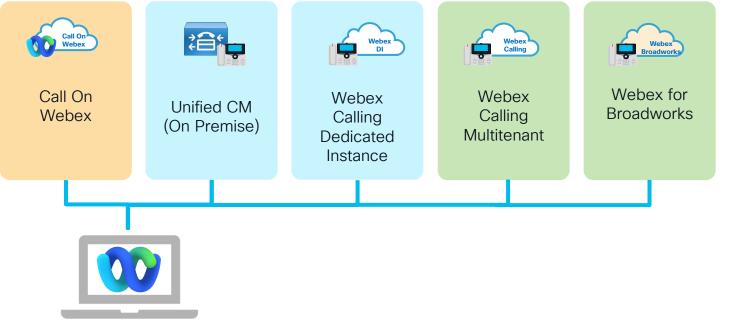- Webex App for Mac and mobile can mark audio, video and screen share packets with appropriate DSCP markings as default

Action
Update any Webex Group Policy to allow DSCP markings for CiscoCollabHost.exe

Calling

Webex App Calling

Call On Webex

Unified CM (On Premise)

Webex Calling Dedicated Instance

Webex Calling Multitenant

Webex for Broadworks

Webex provides flexible calling deployment models to meet your organizations needs

Webex App Calling

Calling experience is defined via user licensing

Call on Webex
- Basic and free 1:1 in-app calling service
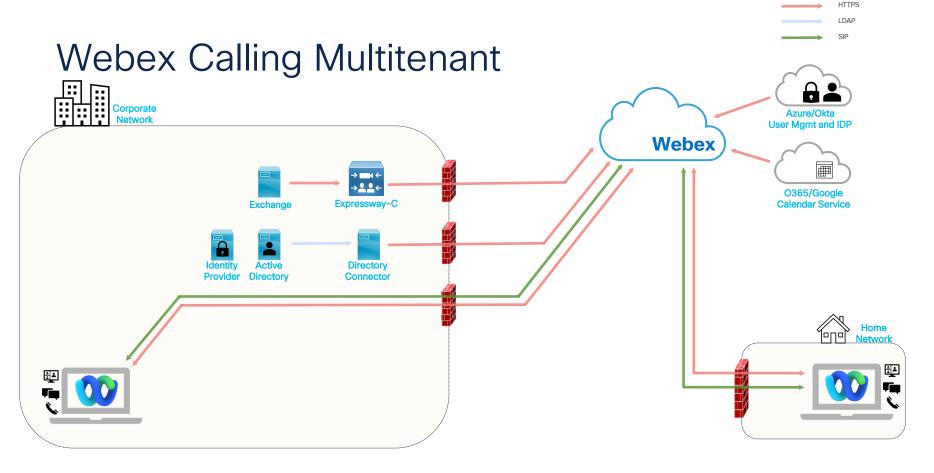- On by default

Register to Unified Communication Manager
- Unified CM on-premise
- Webex Calling Dedicated Instance

Webex Calling
- Webex Calling Multitenant

Webex for Broadworks is managed by your Service Provider

Webex Calling Multitenant

Webex Calling Multitenant

A partial list of supported calling features

Alternate numbers	Call logs w/click to dial	Directed call pickup	Inbound caller ID	Pre-alert announcement	Simultaneous ring
ATA support	Call redial	Directed call pickup barge in	Inbound fax to email	Privacy	Speed Dial 100
Auto attendant	Call restrictions	Distinctive ring	Main number outbound call ID	Webex Go	T-38 Fax
Barge-in exempt	Call routing and queuing	Do not disturb	Mobility	Reports and metrics	Three-way calling (variable length)
Business continuity (CFNR)	Call transfer – attended	Enterprise phone directory	Music on hold (site)	Receptionist client	Video (point to point)
Busy lamp monitoring	Call transfer-blind	Exec / assistant	N-Way voice and video calling (6)	Schedules	Virtual extensions
Call forwarding	Call waiting – Up to 4 calls	Feature access codes	Single number reach (Office anywhere)	Selective call rejection	Visual voicemail
Call history	Conferencing (site based)	Hoteling (guest)	Outbound caller ID blocking	Sequential ring	Voicemail transcription
Call hold and resume	Convenience call recording	Hunt group	Personal phone directory	Shared line appearance	Video N Way

Webex Calling Multitenant
App Configuration

Numbers
- Acquire phone numbers for your organization

Virtual Lines
- Configure multiple lines/shared lines (up to 8 lines. Desktop only, mobile coming soon

Features
- Configure calling features such as Call Queues, Hunt Groups, Call Pickup, Call Park

Service Settings
- Configure services such as E911 settings, Call Recording, Business Texting, Voicemail etc

Client Settings
- Configure the App In-Call feature access as well as MS Teams integration settings

Webex Calling Multitenant

Client Settings

Remember
You can use templates to manage Client Settings for different groups of users

Call Settings
- Control how calling options are displayed when a user selects to make an audio or video call. Remove a calling option that you do not want to present to your users (e.g. Call on Webex)

In-call feature access
- Control mid call settings
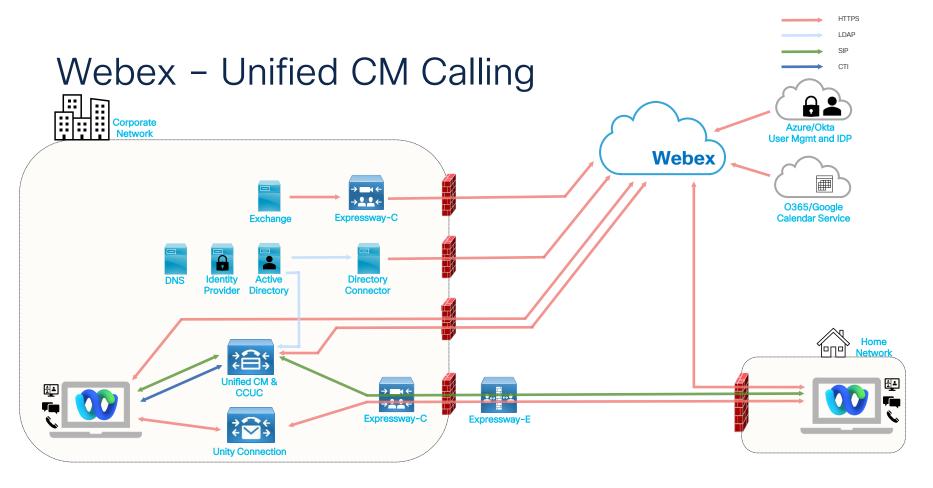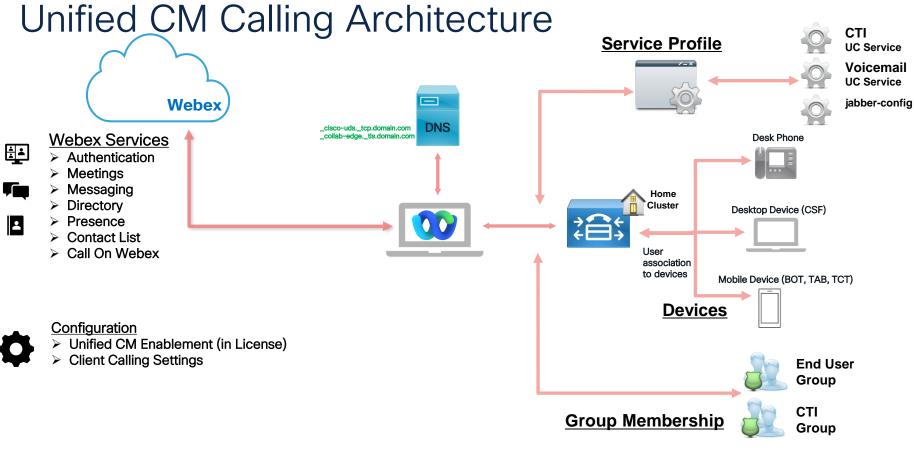
Microsoft Teams integration
- Configure MS Teams integration features such as presence interop

Do Not Disturb (DND) status sync
- Enable/Disable synchronization between deskphone and Webex App DND

Webex – Unified CM Calling

Unified CM Calling Architecture

Webex

Webex Services
- Authentication
- Meetings
- Messaging
- Directory
- Presence
- Contact List
- Call On Webex

Configuration
- Unified CM Enablement (in License)
- Client Calling Settings

_cisco-uds._tcp.domain.com
_collab-edge._tls.domain.com

DNS

Service Profile

CTI
UC Service

Voicemail
UC Service

jabber-config

Home Cluster

User association to devices

Desk Phone

Desktop Device (CSF)

Mobile Device (BOT, TAB, TCT)

Devices

End User Group

CTI Group

Group Membership

Cloud-Connected UC (CCUC)

Analytics

Troubleshooting

Operations Dashboards

Certificate Management

Web RTMT

Borderless CTI

Rich Presence

Touchless Provisioning Webex App

Directory Svc Azure AD Support

MS Teams Integration

Migration & Deployment Insights

Unified CM

Unified CM IM & Presence

Unity Connection

Cisco Emergency Responder

Endpoints & Headsets

Provisioning

- User Provisioning
- Unified CM Device Provisioning

Calling Features

- Phone Presence for Webex App
- Borderless CTI

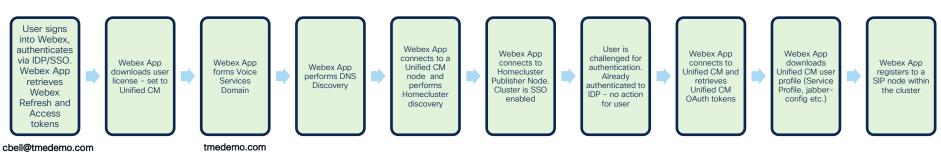## Microsoft Teams Integration

- Call History
- Voicemail (Unity Connection)
- Presence Sync – Webex <-> Microsoft

Unified CM Calling First Time Sign In
Unified CM On-Premise and Webex Calling Dedicated Instance

| User signs into Webex, authenticates via IDP/SSO. Webex App retrieves Webex Refresh and Access tokens | → | Webex App downloads user license - set to Unified CM | → | Webex App forms Voice Services Domain | → | Webex App performs DNS Discovery | → | Webex App connects to a Unified CM node and performs Homecluster discovery | → | Webex App connects to Homecluster Publisher Node. Cluster is SSO enabled | → | User is challenged for authentication. Already authenticated to IDP - no action for user | → | Webex App connects to Unified CM and retrieves Unified CM OAuth tokens | → | Webex App downloads Unified CM user profile (Service Profile, jabber-config etc.) | → | Webex App registers to a SIP node within the cluster |

cbell@tmedemo.com   tmedemo.com

Voice Services Domain
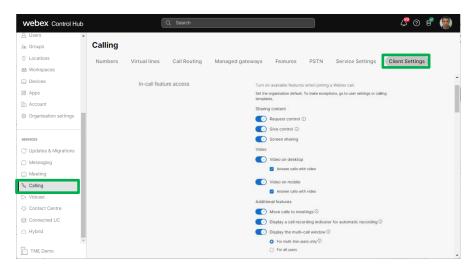RHS of email address entered in the Webex App first screen or domain name specified by admin in Control Hub

DNS Discovery
Webex App sends 2 DNS SRV queries to locate Unified CM or Expressway-E
_cisco-uds._tcp.*tmedemo.com*
_collab-edge._tls.*tmedemo.com*

Homecluster Discovery
Process to find the users cluster in a multi cluster Unified CM deployment. Webex sends 2 queries to Unified CM using the email address the user entered in the Webex App first screen e.g. cbell@tmedemo.com
https://*ucmFQDN*:8443/cucm-uds/clusterUser?**username=cbell**
https://*ucmFQDN* :8443/cucm-uds/clusterUser?**email=cbell@tmedemo.com**

Unified CM Calling Configuration
Control Hub

Call Settings
• Control how calling options are displayed when a user selects to make an audio or video call. Remove a calling option that you do not want to present to your users (e.g. Call on Webex)

Calling Behavior
• Manage UC Profiles to configure a Voice Services Domain

Unified CM Settings
• Option to disable Webex App certificate validation
• Enable automatic Unified CM device provisioning (via CCUC)

Unified CM SIP Address Routing
• Control how SIP URI calls are routed
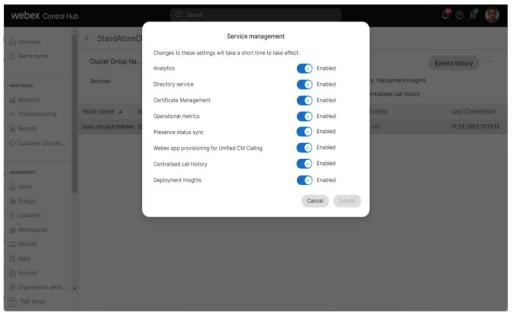
In-call feature access
• Control mid call settings

Microsoft Teams integration
• Configure MS Teams integration features such as presence interop (via CCUC)

Do Not Disturb (DND) status sync
• Enable/Disable synchronization between deskphone and Webex App DND (via CCUC)

Unified CM Calling Configuration
Cloud Connected UC

Cloud Connected UC is highly recommended for deployments

- Webex App Unified CM Calling
- Webex App with Webex Calling Dedicated Instance (CCUC is installed by default)
- Jabber to Webex App migrations
- Webex Calling for MS Teams

Unified CM Calling Configuration
User and Device Configuration

User

The user will use their email address or UPN to sign into Webex App. Webex App will use this address to locate user in Unified CM

e.g. sign into Webex App with
cbell@tmedemo.com

Unified CM user account must have one of the following attributes matched

User ID: *cbell*
Mail ID: *cbell@tmedemo.com*

Service Profile

Voicemail

Voicemail Profile		
Primary	ucxn-pub.tmedemo.com	
Secondary	ucxn-sub.tmedemo.com	
Tertiary	<None>	
Credentials source for voicemail service*	Not set	

Deskphone Control Mode

CTI Profile	
Primary	cm-sub1
Secondary	cm-sub2
Tertiary	cm-pub

Calling Feature Configuration

Jabber Client Configuration (jabber-config.xml) Profile	
Common	common01-webexapp
Desktop	<None>
Mobile	<None>

Device

Platform	Device Type
Windows	CSF
Mac	CSF
Linux	CSF
VDI	CSF
iPad	TAB
Android Tablet	TAB
Chromebook	TAB
iPhone	TCT
Android Phone	BOT

Unified CM Calling Configuration
Webex App will use the Jabber Client Configuration

Any Jabber parameters that are not applicable to the Webex App will be ignored

Parameter	Description and Values	Supported platforms
E911EdgeLocationWhiteList	**Parameter:** E911EdgeLocationWhiteList Specifies a whitelist of up to 30 Service Set IDs (SSIDs) separated by a semicolon. You must configure this parameter when the E911EdgeLocationPolicy parameter is set to true. Then the client monitors users who connect to the corporate network through Expressway for Mobile and Remote Access network. Example:	Desktop and mobile
EnableCallPark	**Parameter:** EnableCallPark Specifies whether the call park feature is available in the client. To access the call park feature, users can choose the More option in the call window. • **true** (default)—Call park is enabled. • **false**—Call park is disabled. There is no call park option under the More button.	Desktop
EnableCallPickup	**Parameter:** EnableCallPickup Specifies if a user can pickup a call in their call pickup group. • **true**—Enables call pickup. • **false**—Disables call pickup (default).	Desktop and mobile

See Deployment guide for Calling in WebexApp (Unified CM) for a full list of parameters

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide.pdf

Webex App Subsequent Logins
Webex OAuth

Default refresh token TTL: 60 days

At initial login, the Webex authorization service issues the Webex App OAuth refresh and access tokens
The access token is used to access Webex services

- The refresh token is used to fetch a new access token at regular intervals.
- The refresh token is stored securely on the Webex App device

This will allow the App to access Webex services across sessions, without the user having to authenticate each time

Once the refresh token expires, the user will need to re-authenticate

Admin can choose to auto extend the refresh token each time the user has a Webex App session

- If the user uses the app before the refresh token expires, the user will not have to reauthenticate
- NOTE: Auto extend is off by default for desktop and mobile

Webex OAuth tokens will allow the App to access Webex services only – Unified CM family OAuth is seperate

Webex App Subsequent Logins
Unified CM OAuth

Default refresh token TTL: 60 days

As the Webex App logs into Unified CM, Unified CM will issue the App with refresh and access tokens.

This will allow the App to access Unified CM services across sessions without the user needing to authenticate with Unified CM each time

NOTE: OAuth refresh token flow is disabled by default and will need to be enabled for the best experience

Unified CM, Unity Connection and Expressway are all part of the same OAuth. OAuth refresh token flow should be enabled on all these platforms

Webex App Subsequent Logins
Unified CM OAuth

Unified CM/Webex App now can auto extend the Unified CM OAuth refresh token

Webex App will auto refresh the refresh token after 50% of the tokens' lifetime
- The refresh should never expire as long as the Webex App is active inside the tokens 50% timeline
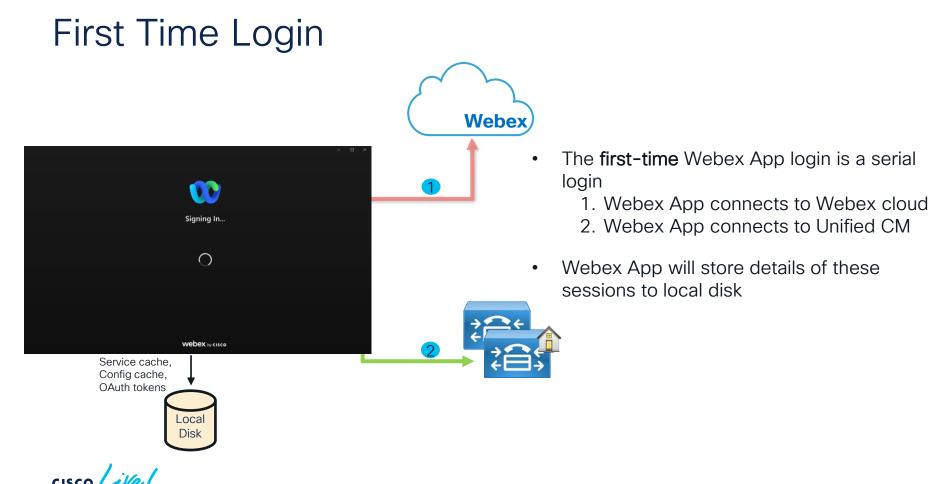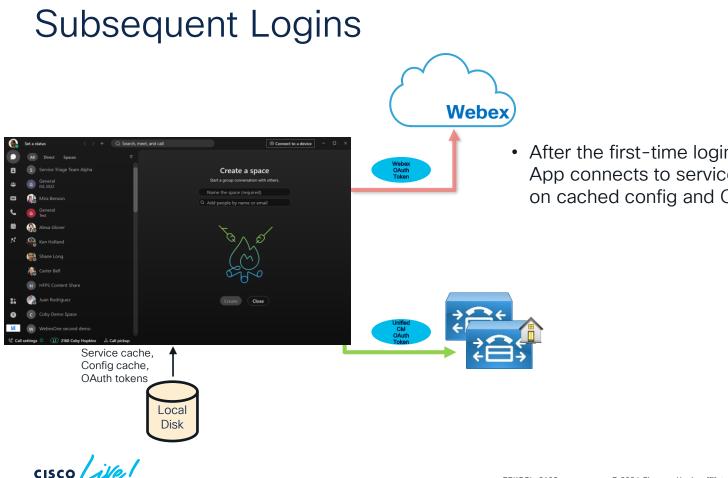
EXAMPLE: If the Unified CM refresh token TTL is set to 60 days, the Webex App will renew for another 60 days, as long as the Webex App is active between day 30 and 60

Requirements
- Unified CM 14.0 SU4 or Unified CM 15
- Expressway X14.3.1
- OAuth Refresh Token flow and Auto Renew Refresh token must be enabled

First Time Login

Signing In...

webex by cisco

Service cache,
Config cache,
OAuth tokens

Local Disk

Webex

① ②

- The **first-time** Webex App login is a serial login
    1. Webex App connects to Webex cloud
    2. Webex App connects to Unified CM

- Webex App will store details of these sessions to local disk

Subsequent Logins

Webex

Webex OAuth Token

Service cache,
Config cache,
OAuth tokens

Local Disk

Unified CM OAuth Token

- After the first-time login on a device, Webex App connects to services in **parallel** (based on cached config and OAuth tokens)

Calling Redundancy

Webex

Service cache,
Config cache,
OAuth tokens

Local Disk

Unified CM OAuth Token

Subsequent logins
- If Webex services are inaccessible (e.g. WAN outage, loss of internet access), Webex App will still be able to register to Unified CM for calling

- Features dependent on Webex services will be unavailable at the time e.g. presence, directory search (previous directory lookups will be cached locally)

Demo

Feature parity

Webex App has surpassed feature parity with Cisco Jabber for most knowledge

		Webex App (Unified CM)	Cisco Jabber
Messaging	IM-only Share	✔	✔
	Remote Desktop Control (Mouse & Keyboard)	✔	✔
Device	Desk-phone Control	✔	✔
Calling	HD Video & Audio Softphone	✔	✔
	Contacts (Corporate, Personal, Local Search)	✔	✔
	In-a-call Presence, DND	✔	✔
	Hold/Resume, Consultative Transfer, Conference	✔	✔
	Call History	✔	✔
	Voicemail (Visual & MWI & Call VM)	✔	✔
	Hunt Group	✔	✔
	Call Pickup	✔	✔
	Call Park	✔	✔
	Extend & Connect & Dial-via Office	✔	✔
	In-Call Sharing	✔	✔
	Call Recording	✔	✔
	Multi-Line	✔	✔
	FECC (Far End Camera Control)	✔	✔
	ICE Media Optimization	✔	✔
	3rd Party Headset Control	✔	✔
	CTI-Control by Other Application	✔	✔
	Enterprise Contact Center (UCCE/X) Support	✔	✔
	Virtual Desktop Integration (VDI)	✔	✔

Incremental features in Webex App

Calling
- Virtual & custom background
- Noise removal and music mode
- Remote side (PSTN) noise removal
- Local push notifications
- Business texting
- Multi call window
- Seamless call handover between networks (Wi–Fi, LTE/4G)
- B2B2C app-to-app calling with annotation and whiteboard
- Move call to meeting
- E911 RedSky native support
- App share with desk phone control
- Desk phone control over MRA
- Whisper coaching
- Barge in for shared line
- Realtime closed captions and translation

Messaging
- Group chat escalation to meeting

Admin/Deployment
- Cisco headset management
- App auto update
- Auto device provisioning
- Epic Rover integration

Device Integration
- Proximity pair with Joining Meeting and 1:1 calling
- Seamless move between device and Webex App
- Wireless share & whiteboard with cloud devices
- 3rd party headset control on Mac
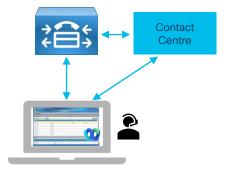- Cisco headset control

End User Experience
- Single app for calling and meetings

Contact Centre features in Webex App

Contact Centre

- Control Webex App via CC application
- Suppress Webex App call window
- Multi Call Window
- Hold/resume
- Transfer
- Conference
- DTMF
- Recording (BIB)
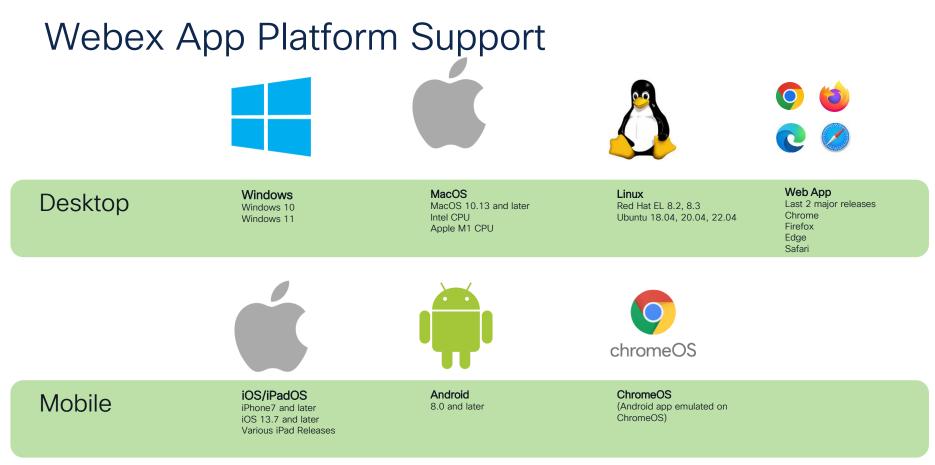- Multi-line
- Call notification control for admin

- Silent monitoring
- Call windows control for user and admin
- Zip tone for auto pickup
- Whisper announcements
- cBarge
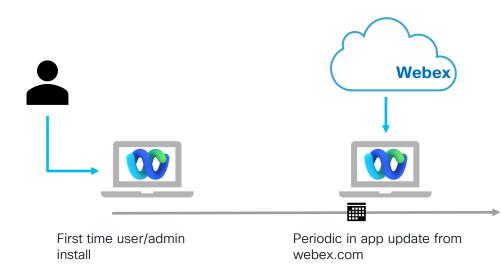- Agent greetings
- Whisper coaching

Contact Centre

App Deployment

Webex App Platform Support

Desktop	Windows	MacOS	Linux	Web App
	Windows 10 Windows 11	MacOS 10.13 and later Intel CPU Apple M1 CPU	Red Hat EL 8.2, 8.3 Ubuntu 18.04, 20.04, 22.04	Last 2 major releases Chrome Firefox Edge Safari

Mobile	iOS/iPadOS	Android	ChromeOS
	iPhone7 and later iOS 13.7 and later Various iPad Releases	8.0 and later	(Android app emulated on ChromeOS)

Webex App Release Cycle

First time user/admin install

Periodic in app update from webex.com

- A new major release of Webex App is delivered monthly
- App versioning is based on time e.g. January 2024 release 44.1.0.28423
  - **Year** : **44**.x.x.xxxx
  - **Month** : 44.**1**.x.xxxxx
  - **Build** : 44.1.**0.28423**

- Webex App monthly release is typically delivered on the first Tuesday of the month
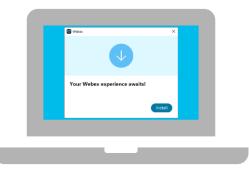 - App auto update may take a number of days to occur after release

Update Management
- Desktop Update Schedule: Control Hub
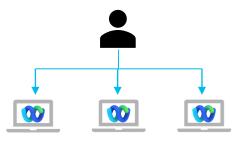- Mobile Update Schedule: App Store Setting

Webex App for Windows

User Install

- User downloads the .exe installer from Webex.com
- Runs the installer
- Webex App is installed to USER PROFILE C:\users*userID*\AppData\Local\CiscoSparkLauncher
- Admin permissions **NOT** required

Admin Install

- Admin installs the Webex App msi installer to Windows machines via deployment tool (e.g. SCCM)
  - msiexec /i webex.msi ALLUSERS=1 /quiet
- Webex App installed to C:\Program Files\Cisco Spark\
- Admin permissions required

Webex App for Windows Installation

- Installer switches can be set to configure the first time experience as well as enabling Outlook integration

Switch	Purpose
ALLUSERS=1	Admin install to C:\Program Files\Cisco Spark\
ACCEPT_EULA=true	Automatically accept EULA so user does not have to
AUTOSTART_WITH_WINDOWS=true	App auto starts on Windows login. User cannot change within the app
DEFAULT_THEME="Light"	Sets theme to light. User can set their preference in the app
DELETEUSERDATA=1	Removes all existing cache is app is already installed
EMAIL=$mail	Prepopulates the Webex App with user email for login (retrieved from AD). Restricts access to the app current Windows user only
ENABLEOUTLOOKINTEGRATION=1	Enables Outlook integration at install time (registry key). Admin permissions required. On by default

Example Webex App for Windows Installation

Example Installation

msiexec /i Webex.msi ALLUSERS=**1** ACCEPT_EULA=**true** AUTOSTART_WITH_WINDOWS=**true** EMAIL**=$mail**
/quiet

- Webex App autostarts with Windows login ✓
- User email is automatically populated ✓
- EULA is accepted ✓
- Next step is authentication…

Consider implementing a seamless authenticating mechanism such as Kerberos

Update Management Setting

- Webex App for desktop software update cadence is set in Control Hub
  - Default is automatic (monthly)

- Organizations can request that Slow channel option is enabled (Only available upon request)

- Software update cadence is an org wide setting. Individual users update cadence can be overridden
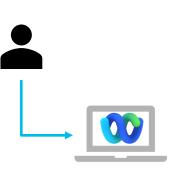
Did you know?

Recurring software updates for the Webex app

Current version: January-2024

Updated on: 11/01/2024

Download Webex builds

Update automatically with every new version, or schedule updates by cadence and deferment. **Learn more**

- ○ Automatic updates (controlled by Cisco)
- ○ Customised scheduled updates with deferrals
- 📅 The next scheduled update is on 06/02/2024 to version February-2024.

Windows App for Windows Update Process

Webex

First time admin install

- msiexec /i webex.msi ALLUSERS=1 /quiet
- Webex App installed to "C:\Program Files\Cisco Spark"
- **CiscoCollabHost.exe** is the main Webex binary running from C:\Program Files\Cisco Spark\

Auto Update

- Webex App downloads update from webex.com
- Update package written to the user profile *C:\users\userID\appdata\local\CiscoSparkLauncher*
- The main Webex binary **continues to be CiscoCollabHost.exe running from C:\Program Files\Cisco Spark** (the original install)
- The auto update process does not reinstall the app – it's simply an update package downloaded to the %appdata% directory, that is loaded at runtime by CiscoCollabHost.exe
- **No admin permissions are required to autoupdate**

Webex App Version Inventory
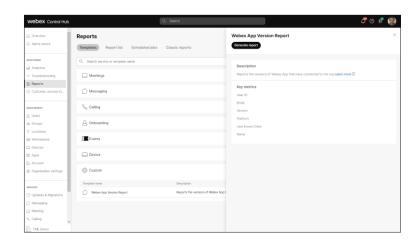
Windows Software Inventory
- Windows software inventory tools typically retrieve the installed app version from a registry key
- Webex App will only write to the registry at first time install
- Software inventory tools may report the first time install version of Webex App (not the active version based on automatic update)
- The latest app version on a Windows machine is written to *C:\users\userID\appdata\local\CiscoSparkLauncher\version.txt*

- Software inventory tools can use this file to determine latest active version of Webex App on the machine

Control Hub Reports
- Create a Report to retrieve the versions of Webex App active in the organization
- Report can be customized to display specific details
- Report will detail users/versions who have connected to the Webex org

Admin Managed Webex App for Mobile Deployment

Webex for Intune

- Webex for Intune allows in app enforcement of policies pushed to a mobile device by the admin e.g.
  - VPN on demand
  - Conditional Access
  - Disable copy/paste

AppConfig

- Webex App for iOS/Android supports AppConfig derived policies
- Policy can be pushed to Webex via an AppConfig compliance EMM e.g. Cisco Meraki, MobileIron etc
- Many policies can be set which will be adhered to by Webex e.g.
  - Disable copy/paste
  - Disable screen capture
  - Login Hint

App Wrapping

- Admins can obtain the Webex App iOS (ipa) and Android (apk) installer files from Cisco
- Admins can then wrap the Webex App installer using their own MDM process and push to mobile devices
- NOTE: Any discovered issues will need to be reproduced using an app store Webex App installer to gain support from Cisco

Webex Network Requirements Tool

https://help.webex.com/nrt

- Define what Webex/3rd party services your Webex App users will consume
- Tool generates a report detailing the network requirements specific to your deployment

Messaging Demo

CISCO *Live!*

CISCO *Live!*

Let's go