CLIENTS

Transitioning from Jabber to Webex

Deployment Guide

September 28, 2021

Contents

What's New in This Guide

Table 1 provide a historical list of updated and new topics added to this guide.

Table 1. *Jabber to Webex Transition Deployment Guide Publication History*

Date	Updated or New Topics	Update Details and Location
January 13, 2021	*Initial document publication*	*Initial release*
January 20, 2021	*Topics throughout document*	*Added documentation references to point to new relevant documents.*
September 29, 2021	*Topics throughout document*	*Product reference name change from "Cisco Webex" to "Webex"*

Introduction

This document will assist in understanding the transition path from Cisco Jabber to Webex. This will cover general considerations and deployment steps as you evaluate a transition from a purely on-premises Jabber deployment to a hybrid Webex environment.

General discussions and detailed steps are included here along with links to other documentation where necessary.

Target Audience

This deployment guide is intended to be used by teams who are transitioning from Cisco Jabber to Webex.

With the new Webex, you can call, message, and meet in one inclusive, secure application. This document will focus on Unified Communications Manager (Unified CM) calling within the Webex App, simplifying the migration by utilizing the existing call control used by Jabber today.

Overview

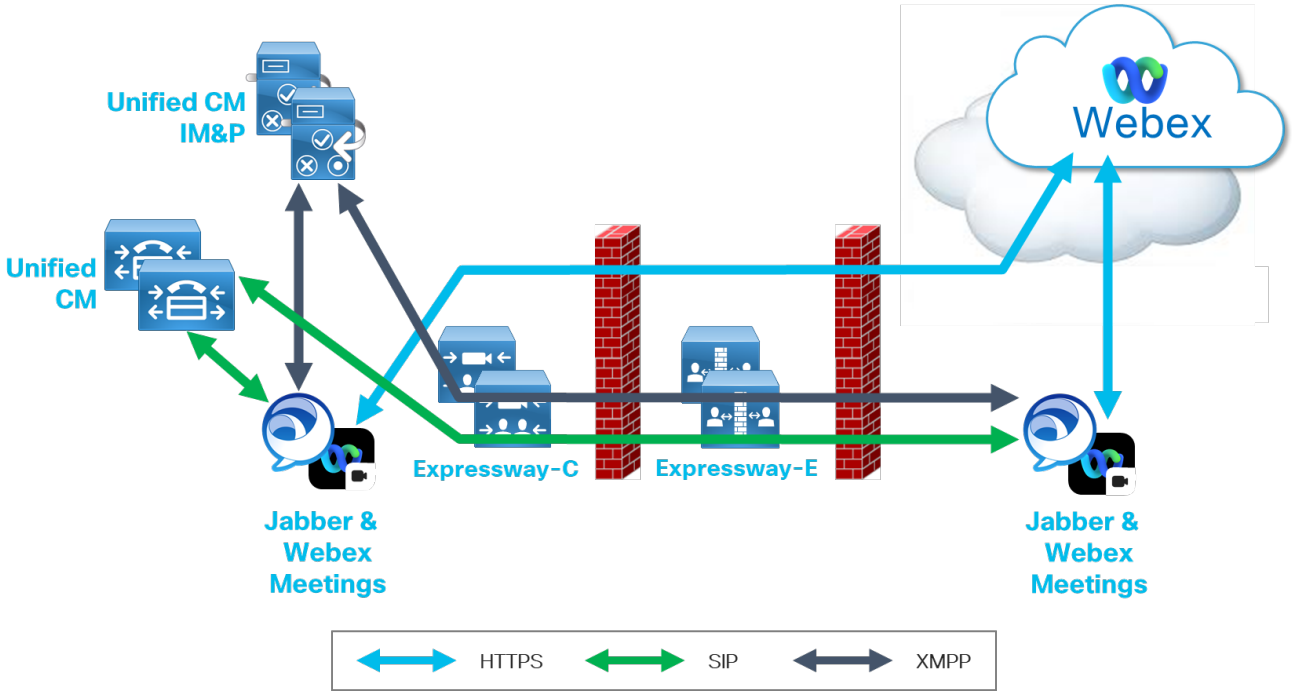
The goal of this document is to assist in the migration from Jabber to Webex. Jabber provides native support for messaging, calling and meetings, however deployment of Jabber for messaging and calling, as well as the Webex Meetings App for meetings, is a very popular deployment model.

The following section details an existing Jabber Full UC deployment with Webex Meetings architecture.

Jabber Full UC Mode with Webex Meetings

Figure 1 below details the architecture for a Jabber Full UC mode with Webex Meetings App deployment. The architecture highlights how Jabber and Webex Meetings applications connect to the services which provide for messaging, calling and meetings modules. The diagram also details the Expressway mobile and remote access architecture, which provides access to calling and messaging services from outside the corporate network boundary.

Figure 1. *Jabber with Webex Meetings Architecture*



Note: The architecture depicted in Figure 1 does not cover voicemail services. Voicemail services delivered via Unity Connection are applicable and will be discussed later in this document. Likewise, the figure does not include important third-party components such directory services, identity providers (IdPs), and so on.

Note: Meeting services may also be supported natively with just the Jabber client. That is Jabber would connect directly to the Webex meetings service instead of having a separate Webex Meetings application. This deployment method while possible is less common than what's shown in Figure 1, but the same transition steps covered later in the document will also apply to that type of deployment.

Table 2 lists the key elements of the on-premises (or hybrid) Jabber Full UC deployment architecture prior to transitioning to Webex.

Table 2. *Before: On-Premises Jabber Deployment Components*

Product	Description
Webex	The Webex platform provides the meetings service to the Webex Meetings App via HTTPS. The Webex Meetings App can be cross launched from Jabber or can be run as a standalone application.
Unified CM	Unified CM provides calling service to Jabber via SIP (softphone mode). Alternatively, Jabber can also connect to Unified CM in deskphone control mode (CTI). Unified CM also provides discovery, configuration, and directory services for Jabber via the UDS service (HTTPS)
Unified CM IM & Presence	Unified CM IM & Presence (Unified CM IM&P) provides messaging and presence service to Jabber via XMPP. Users contact lists are also stored on IM&P.
Expressway-C/E	Expressway-C and Expressway-E provide mobile and remote access (MRA) to Jabber clients running outside the corporate network boundary, allowing Jabber to connect to calling and messaging services.

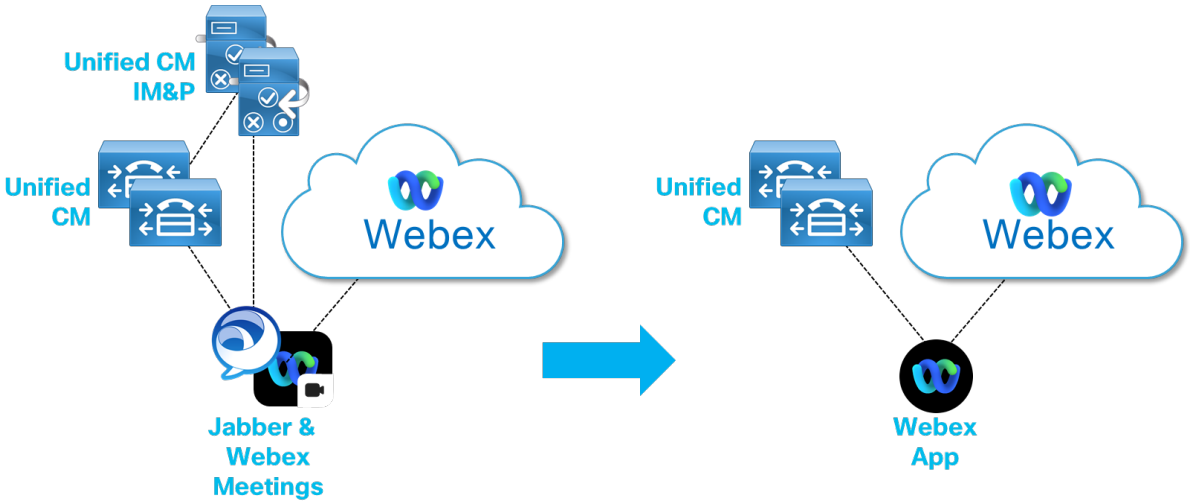
Cisco Jabber may connect to several services depending on the deployment. Services include:

- Calling – Unified CM
- IM and Presence – Unified CM IM&P
- Voicemail – Unity Connection
- Mobile and remote access (MRA) – Expressway
- Meetings – Webex Meetings

Each service has its own interface, but Jabber is primarily managed and configured from Unified CM.

As illustrated in Figure 2, customers who have Jabber may choose to transition this architecture to Webex and cloud-based services, while retaining on-premises Unified CM for device registration and call routing. The decision to make this transition should be made based on customer's functionality requirements.

Figure 2. *Transition Decision: Jabber and Webex Meetings to Webex App*



Customers that have the following conditions should consider carefully before making the decision to embark on this transition:

- Unreliable Internet access.
- Zero chat retention requirement
- Very strict compliance requirements including:
  - Content storage in country (specific to some countries).

Jabber Architecture

Before discussing the target architecture, it's important to understand the existing Jabber deployment. The architecture for Jabber Full UC Mode with Webex Meetings will be used as an example. For other Jabber deployments, messaging and meetings services can be ignored as needed.

There are several aspects to understand about the existing Jabber architecture before migrating to the Webex App.

Service Discovery, Authentication and Configuration

When Jabber starts for the first time, it will run through a process called service discovery. Jabber relies on DNS services to perform service discovery. The purpose of service discovery is to define:

1. Which service Jabber should connect to (sometimes referred to as edge-detection)?
2. The location of the service.

Jabber will send two DNS SRV requests based on the domain name that the user enters on the initial sign in screen, for example, *alice@example.com*. Jabber expects to discover one of the following SRV records in DNS:

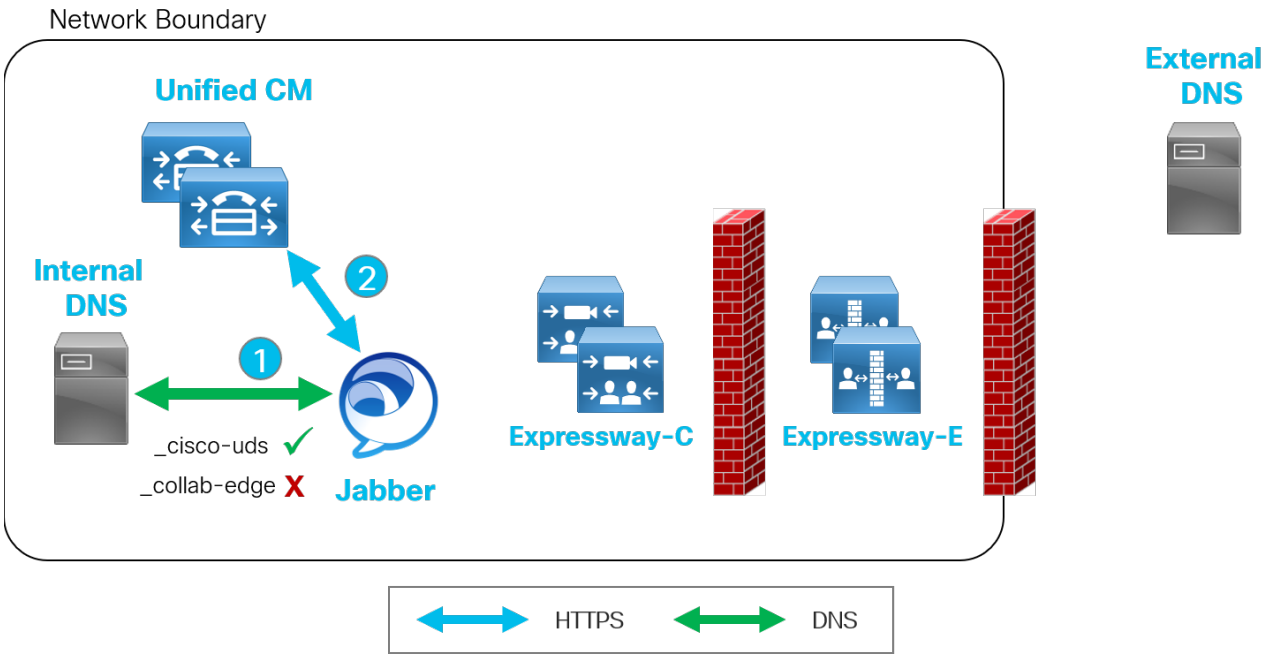
- *_cisco-uds._tcp.example.com*
- *_collab-edge._tls.example.com*

The *_cisco-uds* SRV record is deployed on the internal DNS service, and points to one or more Unified CM nodes. The *_collab-edge* SRV record is deployed on the external DNS service, and points to one or more Expressway-E nodes.

If Jabber discovers a *_cisco-uds* SRV record, Jabber determines that it is located on the internal network and will connect to Unified CM directly. If Jabber discovers a *_collab-edge* SRV record instead of the *_cisco-uds* SRV record, Jabber determines that is located outside the internal network boundary, and will need to connect through Expressway-E, to gain access to internal calling and messaging services.

Figure 3 details how Jabber, located **inside** the corporate network boundary, discovers and makes its initial connection to Unified CM. The *_cisco-uds* SRV record is configured on the internal DNS service.

Figure 3. *On-Premises Jabber Service Discovery*



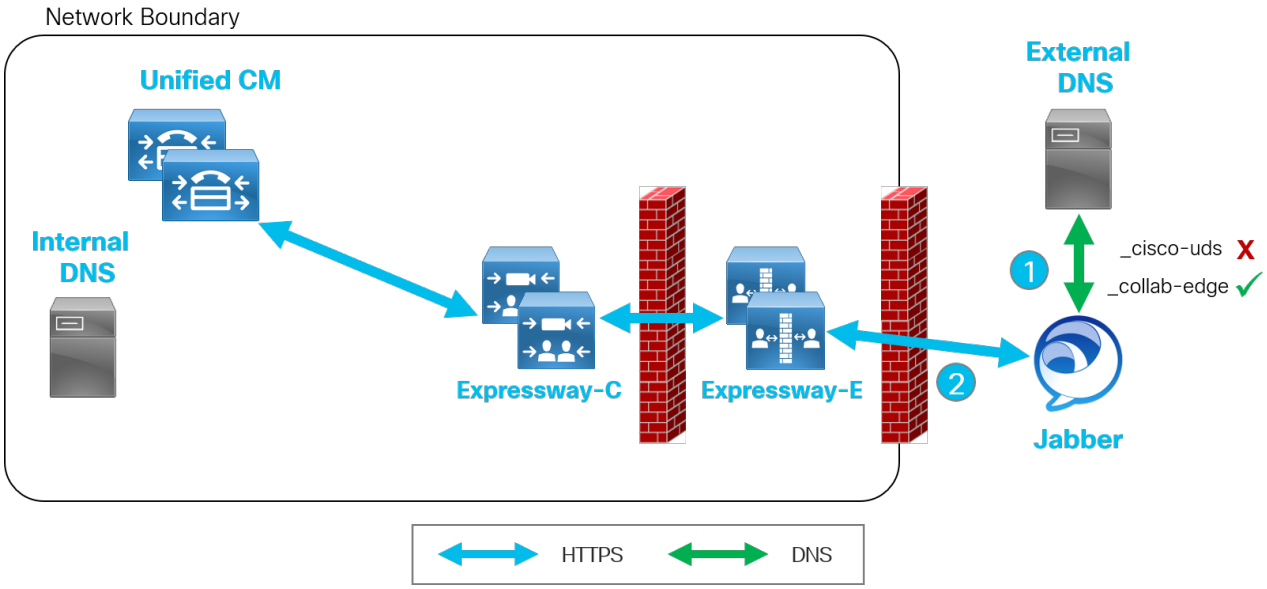
The discovery flow depicted in Figure 3 is as follows:

1. Jabber queries DNS for *_cisco-uds* and *_collab-edge* SRV records. DNS returns a result for *_cisco-uds*. The result is the DNS A record of a Unified CM node within the organization.

2. Jabber makes its primary connection to Unified CM via HTTPS. The primary connection is responsible for determining the software version of Unified CM, as well as initiating home cluster discovery.

Figure 4 details how Jabber, located **outside** the corporate network boundary connecting over Expressway Mobile and Remote Access (MRA), discovers and makes its initial connection to Expressway-E. The *_collab-edge* SRV record is deployed on the external/public DNS service.

Figure 4. *Expressway Mobile and Remote Access Jabber Service Discovery*



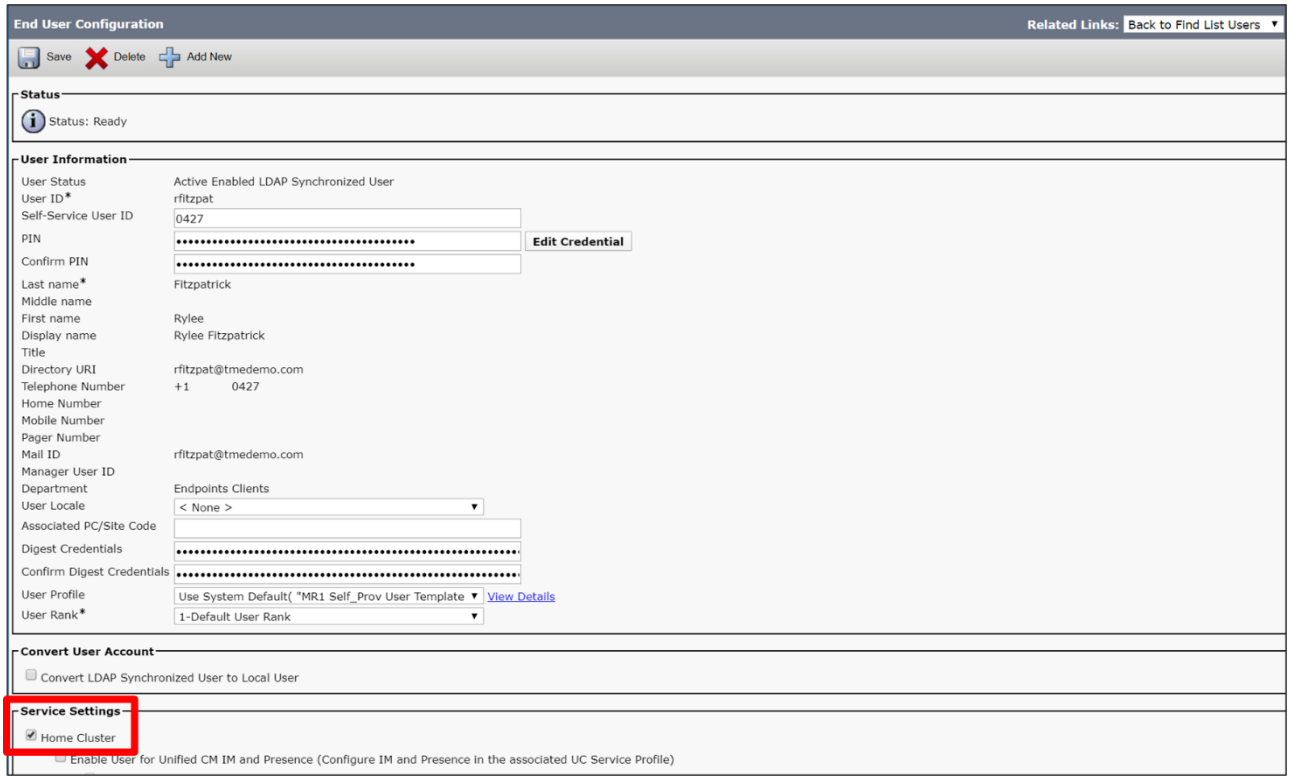
The flow depicted in Figure 4 is as follows:

1. Jabber queries DNS for *_cisco-uds* and *_collab-edge* SRV records. The external DNS service returns a result for *_collab-edge*. The result is a DNS A record for an Expressway-E node within the organization.

2. Jabber makes its primary connection to Expressway-E via HTTPS. The primary connection will typically involve authentication as well as a configuration request. Expressway-E will then pass the request to Expressway-C, which will initiate home cluster discovery against Unified CM on behalf of the Jabber client.

Home cluster discovery is the process whereby Jabber makes its primary connection to any Unified CM node in the organization and then is redirected to the publisher node of the user's assigned home cluster. The user's home cluster is the cluster where the user will obtain services for configuration download, device registration, deskphone control mode, search, and so on. A user's home cluster is defined when the administrator associates the user with a particular home cluster. Home cluster can be set in bulk (for example with the BAT tool) or manually on a per user basis at the end user page. Figure 5 shows the *Home Cluster* checkbox is checked for a user on this cluster.

Figure 5. *Unified CM: End User Home Cluster Setting*



Home cluster discovery relies on the Intercluster Lookup Service (ILS). ILS provides several capabilities including the ability for any Unified CM node within the organization, to locate the home cluster of a particular user. ILS should be configured between all Unified CM clusters.

Home cluster discovery as described and shown above also applies to MRA-based remote connections, whereby Expressway-C performs the home cluster discovery on behalf of the remote Jabber client.

Home cluster queries sent by Jabber are as follows:

- https://**UnifiedCM_FQDN**:8443/cucm-uds/clusterUser?username=**alice**
- https:// **UnifiedCM_FQDN**:8443/cucm-uds/clusterUser?email=**alice@example.com**

The *Unified CM_FQDN* component of the above URLs is determined by the Unified CM address returned from the DNS SRV query for *_cisco-uds*.

Note: For Jabber connections over MRA, Expressway-C will perform the home cluster query against the internal DNS server.

The user identifier at the end of the query will be based on what the user types into Jabber on the primary login screen (where the user types in their username and domain, often the users email address). Jabber will send two queries: one using username, and one using email. The reason for the two queries is to cater for organizations who do not standardize on using username as UID in Unified CM.

Note: With Unified CM 10.5.2 and later, users email addresses are synced from LDAP directory during LDAP sync.

Note: Jabber on Windows can read the User Principal Name (UPN) from the local machine and use this to initiate discovery – this will mean that the user will never see the initial Jabber login screen. UPN discovery can be disabled with the following installer switch:

msiexec /i CiscoJabberSetup.msi UPN_DISCOVERY_ENABLED=false CLEAR=1 /quiet

Once home cluster discovery is successful, Jabber will connect to the publisher node of the home cluster and ask for a list of all nodes within the cluster. Jabber will connect to a randomly selected node from the list returned and request the download of user configuration. That Unified CM node will then challenge Jabber for authentication.

Unified CM supports three methods of user authentication:

1. SAMLv2 single sign-on (SSO)
2. LDAP authentication
3. Basic username password

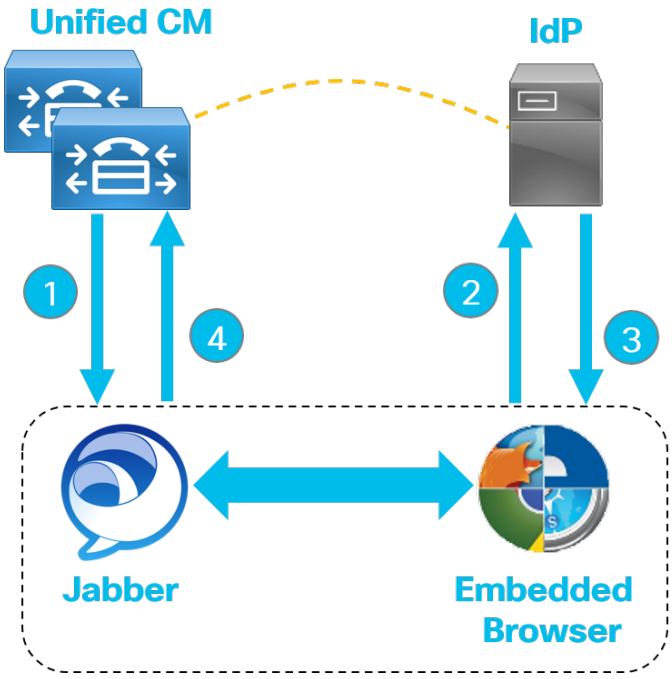
SSO is the preferred method of authentication for Jabber and the Webex App. This document will assume SSO is already enabled for the organization.

When Jabber is challenged for authentication, it is redirected to the identity provider (IdP). The IdP will challenge Jabber for a specific type of authentication, depending on how the IdP is configured. Examples of authentication include username/passwords, Kerberos, certificate authentication, and so on. Jabber will call upon the system browser (embedded browser) to support the authentication request. Depending on the

authentication type enabled, Jabber may display an embedded browser to prompt the user to enter a credential. Once the user authenticates, Jabber will receive a SAML token from the IdP. This SAML token can then be presented to Unified CM, and Jabber will be granted access to Unified CM services.

A high-level flow of this process is detailed in Figure 6.

Figure 6. *Jabber Embedded Browser Flow*



The flow depicted in Figure 6 is as follows:

1. Unified CM is SSO enabled and redirects authentication requests to the IdP.
2. Jabber calls to the embedded browser to connect to IdP and authenticate. User/embedded browser authenticates based on authentication types enabled by the IdP (for example, username/password, Kerberos, or certificate).
3. IdP issues embedded browser a SAML cookie.
4. Jabber uses the SAML cookie to gain access to Unified CM services.

Once Jabber has authenticated with Unified CM, it will retrieve an OAuth refresh token. Jabber will use the OAuth refresh token to retrieve an OAuth access token from Unified CM. The access token will be used to gain access to specific services including UDS, and other services. This flow assumes that OAuth Refresh Token Flow is enabled on Unified CM.

Jabber will then download user configuration including:

- Service profiles
- Jabber configuration
- End user configuration
- Device list
- Device configuration

The service profile defined in Unified CM will detail the subsequent services and the service location (FQDN) that Jabber should connect to if configured. The service profile may include some or all the following services:

- IM and Presence
- Voicemail
- Conferencing
- CTI
- Directory
- Jabber Client Configuration

Jabber connects to IM and presence (Unified CM IM&P), voicemail (Unity Connection), and conferencing (Webex Meetings) services if enabled. Jabber uses the existing SAML token to authenticate against each of these services (assuming each service is SSO enabled).

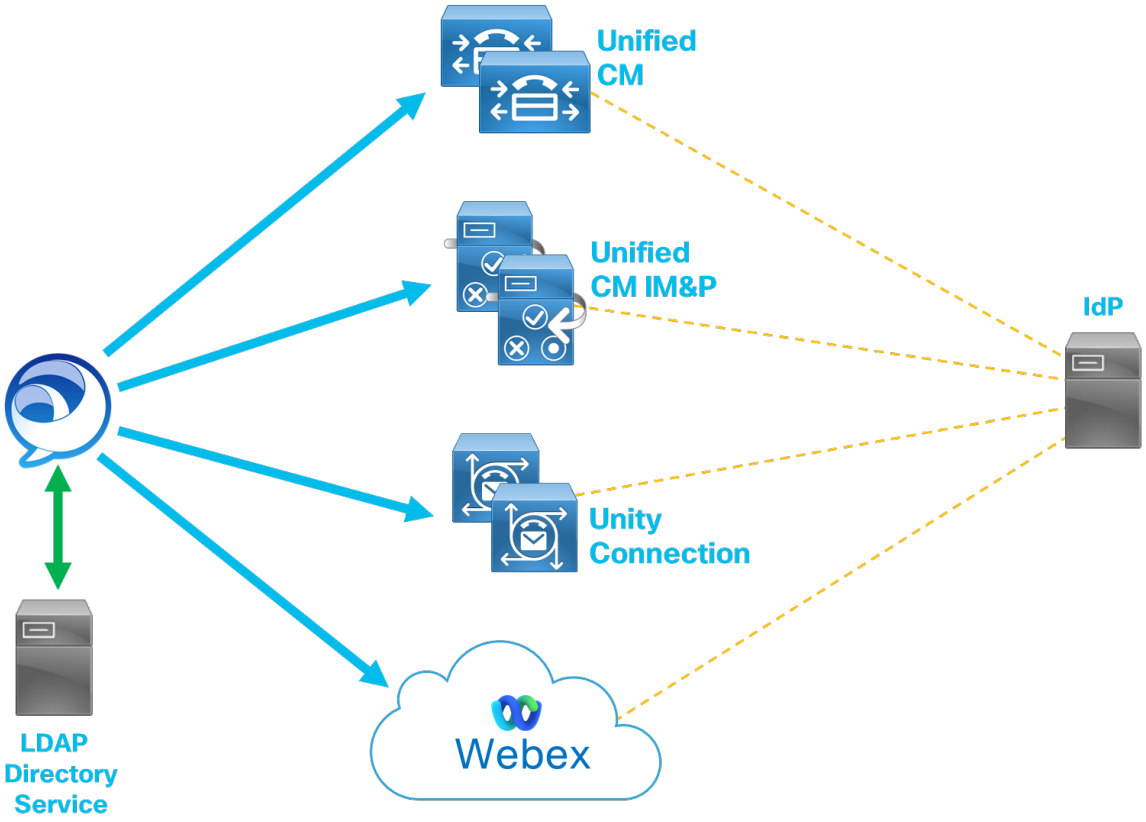
Jabber connects to the CTI service if the user selects to run in deskphone control mode.

Jabber connects to the configured directory service –either an LDAPv3-based directory service (for example, Active Directory) or the UDS directory service running on Unified CM.

Jabber automatically downloads the Jabber client configuration in the case of Unified CM 12.5 and above. This configuration is equivalent to what can be configured in the automatically downloaded jabber-config.xml file with Unified CM 11.5 and earlier.

Figure 7 details how Jabber would connect to all services if configured. SSO enabling all services, allows users to authenticate once, and gain access to different services. If Jabber is running in Phone Only mode for example, the Unified CM IM&P service would not be configured.

Figure 7. *Jabber Services*



Subsequent Logins

Jabber will write service details to a cache file that will be stored on the local device. The service details include the server addresses (for example, the address of Unified CM and Unified CM IM&P nodes) that Jabber last successfully connected to.

Jabber will also store the OAuth refresh token previously retrieved from Unified CM. The OAuth refresh token can be used to retrieve a new OAuth access token, without requiring re-authentication. (This assumes OAuth Refresh Token Flow is enabled on Unified CM, Unity Connection, and Expressway).

After one successful sign in, Jabber will subsequently discover and sign into services based on the details in the cache. Jabber will read the cache, connect to services

defined in the cache, and use the OAuth refresh token to retrieve an access token to gain access to those services. This capability is referred to as Fast Login.

In the first few minutes after connecting to services, Jabber will perform configuration refresh in the background. Jabber will resend DNS SRV queries as well as checking Unified CM for any configuration changes. If a configuration change is detected, the user may be prompted to sign out of Jabber to retrieve the new configuration.

Contact Lists

For Full UC Mode or Phone Only Mode with contacts-based deployments, contact lists are stored on the Unified CM IM&P server. Contact lists will be downloaded at initial login, and users can add or remove persons from their contact lists. Jabber will maintain a copy of the contacts list locally in a cache file. This file is stored on disk, encrypted with tools provided by the local OS (for example, Keychain on Mac). This contact list can be copied to the Webex App during migration. The details of this are discussed later in this document.

Directory Integration

Jabber relies heavily on a directory integration for a consistent user experience. Jabber can integrate directly with an LDAPv3 based directory service (for example, Active Directory) or the UDS directory service running on Unified CM. Jabber relies on the directory integration for several functions including:

- Contact search
- Contact resolution
- Incoming caller resolution

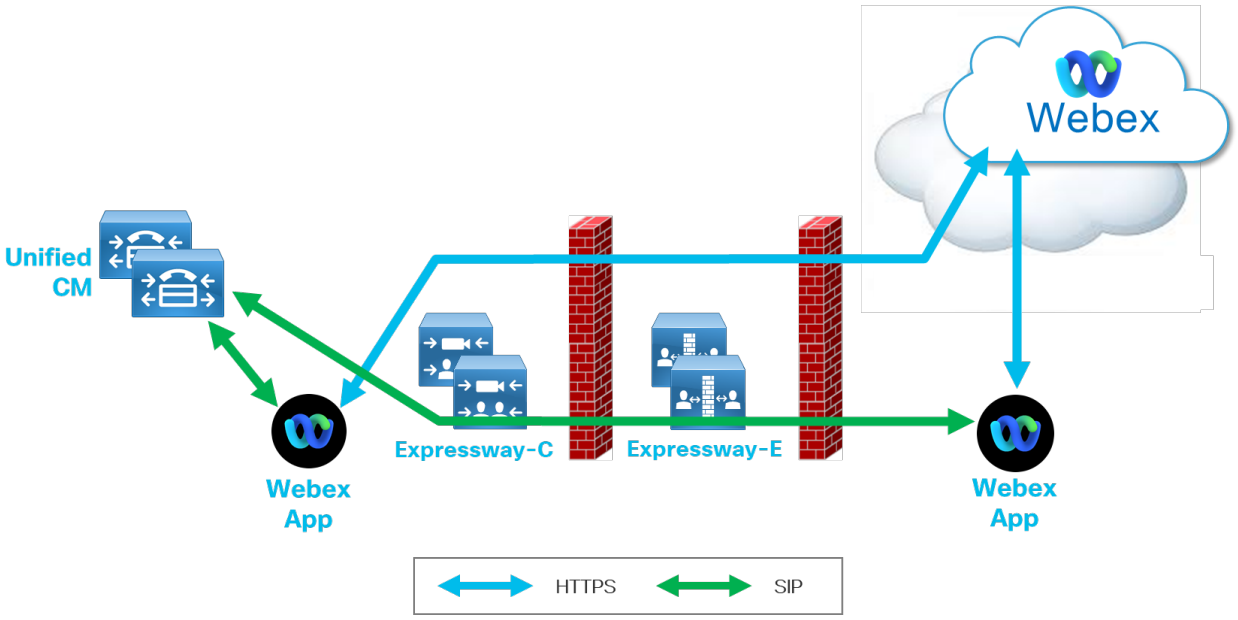
Jabber will always connect to the UDS directory service when connecting over Expressway MRA, while it can connect to LDAP or UDS directory service when connecting from the corporate network. The user data must be consistent across LDAP and UDS to allow for consistent user experience.

Core Components

Roles of the Components Involved

Figure 8 details the target architecture for a Webex App deployment with Unified CM calling. The architecture highlight's how the Webex App connects to services which provide for messaging, calling, and meetings. The diagram also details the Expressway mobile and remote access architecture, which provides access to Unified CM calling services from outside the corporate network boundary.

Figure 8. *After: Webex App with Unified CM Calling Architecture*



Note: Figure 8 does not show important third-party components including directory services and identity providers (IdPs)

Table 3 lists the new elements of the architecture after transitioning to Webex.

Table 3. *After: Webex Infrastructure Components*

Product	Description
Webex	The Webex platform provides the messaging and meetings services to the Webex App via HTTPS. The Webex platform also provides, configuration, entitlements, and directory services for the Webex App.
Unified CM	Unified CM provides calling service to the Webex App via SIP (softphone mode). Alternatively, the Webex App can also connect to Unified CM in desk phone control mode (CTI). Unified CM also provides for service discovery and calling configurations for the Webex App (HTTPS).
Expressway C and E	Expressway C and E provides mobile and remote access (MRA) to Webex running outside the corporate network boundary, allowing the Webex client to connect to calling services.

The Webex App may connect to several services depending on the deployment. These include:

- Webex platform (including messaging and meetings)
- Unified CM
- Unity Connection
- Expressway (MRA)

The Webex App is primarily managed from Webex Control Hub (Control Hub). Control Hub is the management interface for Webex. Control Hub provides administrators with the ability to manage users and configure features and settings for the organization. Control Hub also provides rich analytics and real-time troubleshooting capabilities.

Note: Webex Meetings can be managed from Webex Site Admin or directly via Control Hub, depending on the organizations existing deployment. If Webex Meetings service is managed by Site Admin before migrating to the Webex App, Site Admin can be linked

with Control Hub to ensure consistency of user provisioning as well as bring the benefits of Control Hub analytics and troubleshooting capabilities to Webex Meetings.

Webex Architecture

This section details the architecture for the Webex App with Unified CM calling.

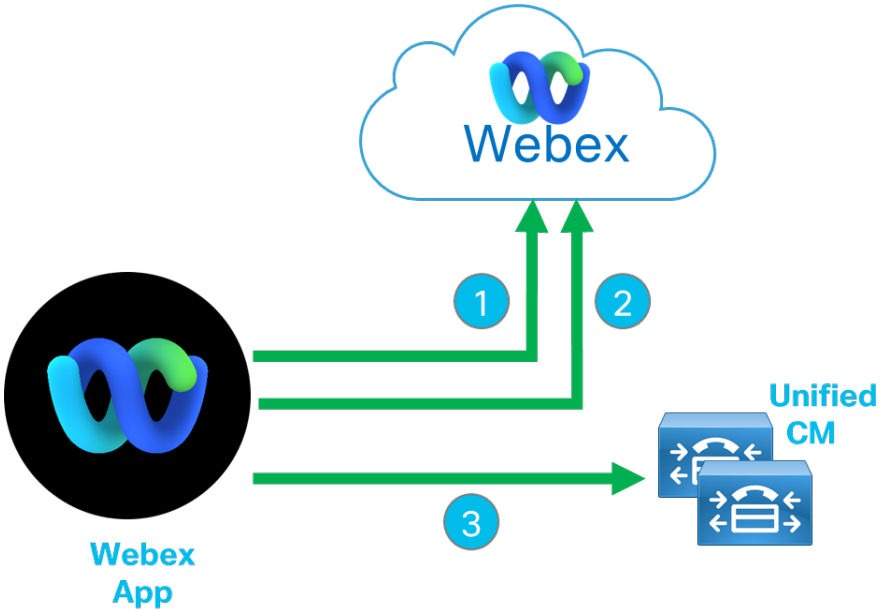
Key aspects of this Webex architecture will be discussed including:

- Service Discovery, Authentication, and Configuration
- Messaging
- Meetings
- Calling
- Subsequent Logins
- Directory Integration

Service Discovery Authentication and Configuration

The high-level flow summary for a first-time login to the Webex App is shown in Figure 9.

Figure 9. *Webex App High-Level Architecture*



The flow depicted in Figure 9 is as follows:

1. User signs into Webex App. User is enabled for Unified CM calling.
2. Webex connects to messaging and meetings services.
3. Webex connects to Unified CM (possibly through Expressway (MRA))

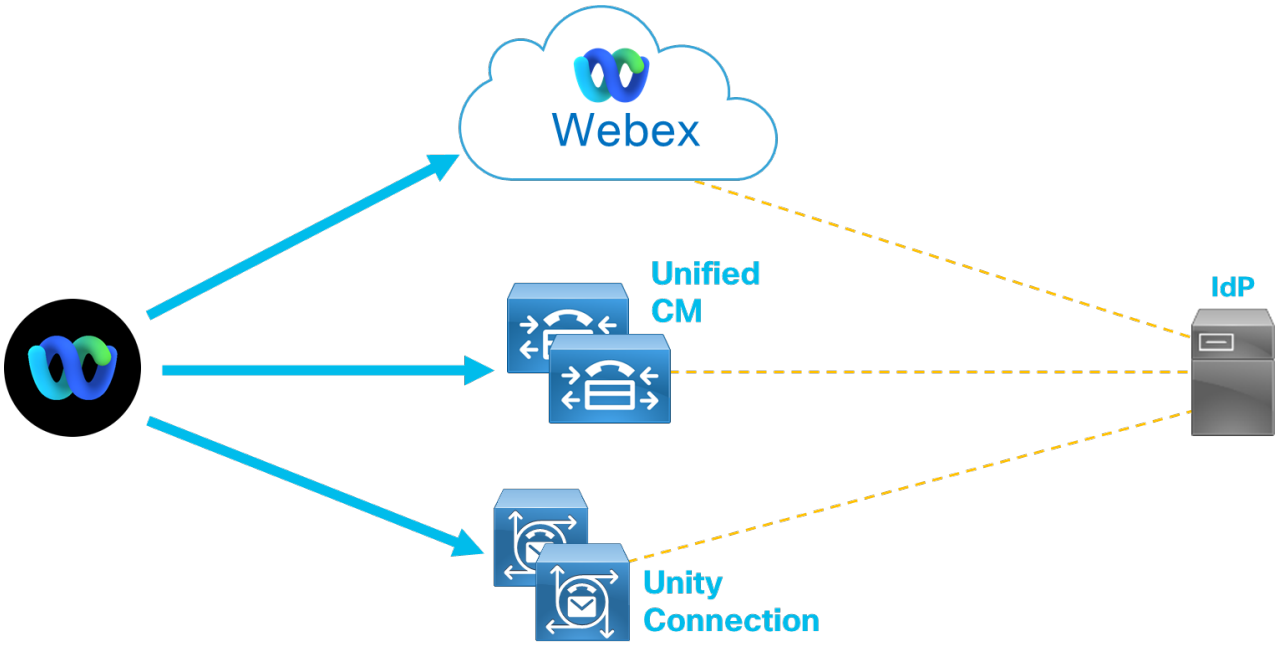
In this section, assume that the following services are SSO enabled:

- Webex Site (Control Hub)
- Unified CM
- Expressway
- Unity Connection

Note: For Webex deployments, SSO is not mandatory, but it is highly recommended to enhance security, and simplify user experience.

Figure 10 shows the Webex App SSO flows.

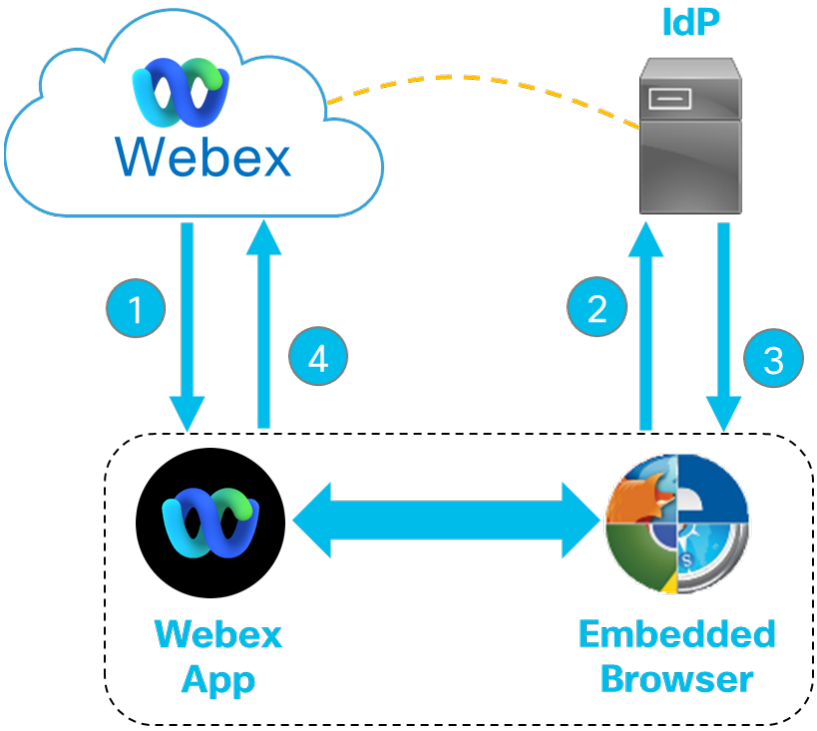
Figure 10. *Webex App SSO*



When the Webex App is launched for the first time, the user will be prompted to enter their email address. Once the user enters the address, the Webex App will connect to the users Webex Site and the user will be challenged for authentication. Assuming the Webex Site is SSO enabled, the Webex App is redirected to the IdP for authentication.

As shown in Figure 11, the Webex App will call upon a system browser/library (embedded browser) to connect to the IdP for authentication.

Figure 11. *Webex App Embedded Browser Flow*



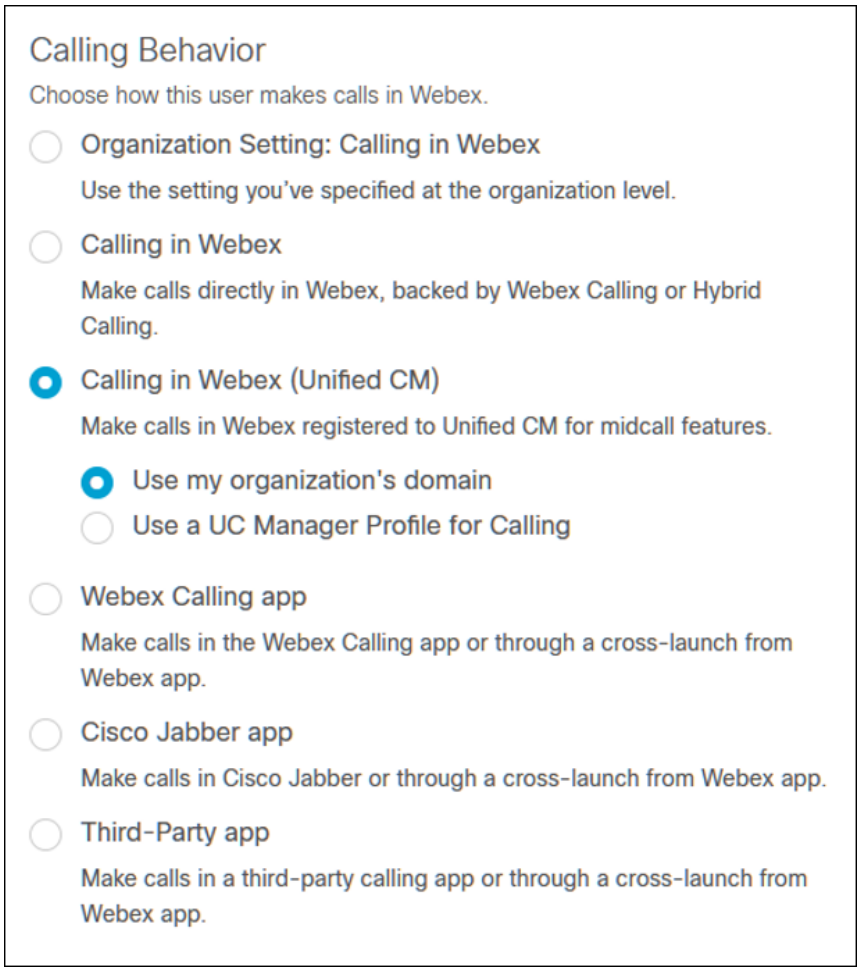
The flow depicted in Figure 11 is as follows:

1. The Webex Site is SSO enabled and redirects authentication requests to the IdP.
2. The Webex App calls to the embedded browser to connect to IdP. The embedded browser/user authenticates based on the authentication type configured by the IdP (for example, username/password, Kerberos, and so on).
3. The IdP issues SAML cookie to the embedded browser.
4. The Webex App then uses the SAML cookie to gain access to Webex services.

Once the Webex App has completed authentication, it will retrieve an OAuth Token that will be used to gain access to Webex services, without the need to authenticate each time. The OAuth token is long life (typically 60 days) and will be stored on the local device for future logins.

The Webex App will next download configuration defining calling behavior. Unified CM Calling behavior is configured in Control Hub. As shown in Figure 12, Unified CM calling behavior is defined using the *Calling Behavior* configuration option, either organization-wide or on a per user basis (manual configuration or in bulk using the CSV file).

Figure 12. *Webex Control Hub: Calling Behavior Configuration*



For up to date information on defining calling behavior refer to the *Deployment Guide for Calling in Webex (Unified CM)* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide.html.

Once calling behavior has been discovered, Webex will then connect to additional services (messaging, meeting, and so on).

Messaging

The Webex messaging service is hosted on the Webex platform. The Webex App connects to the messaging service in Webex. Messaging is configured and managed via Control Hub. Important configurations and policies for Webex messaging include:

- Message and file sharing policy
  - Message retention
  - Messaging compliance
  - Content/File management
- External messaging policy

Webex datacenters will store customer data when using the Webex App. Data stored includes user identities, encryption keys, and user generated content. Organizations can choose which geo-based datacenter their data should be stored. The datacenter should be selected when the Webex Organization is being created.
For more information refer to the *Data Residency in Webex* article available at https://help.webex.com/en-us/oybc4fb/Data-Residency-in-Webex.

Meetings

Webex meetings service is hosted on the Webex platform. Organizations who already utilize Webex Meetings service, can continue to use their existing service with the Webex App. The following configurations are required to utilize existing Webex Meetings Site in the Webex App.

- Linking Site Admin to Control Hub.
- Enablement of Webex Meetings experience in the Webex App.

Calling

The Webex App will connect to a native cloud calling service hosted on the Webex platform. This native calling service provides basic call control and allows Webex App users to call other users who have an account on the Webex platform. It will also allow users make calls via SIP URI to external services. This calling service is also the service that is used when the Webex App dials into a space meeting.

The native calling service does not provide for advanced call features like hold, resume, transfer, and so on, nor does it provide the ability to integrate with a PSTN service. As

such, organizations typically deploy the Webex App with a call control service. The Webex app can integrate directly with the following call controls:

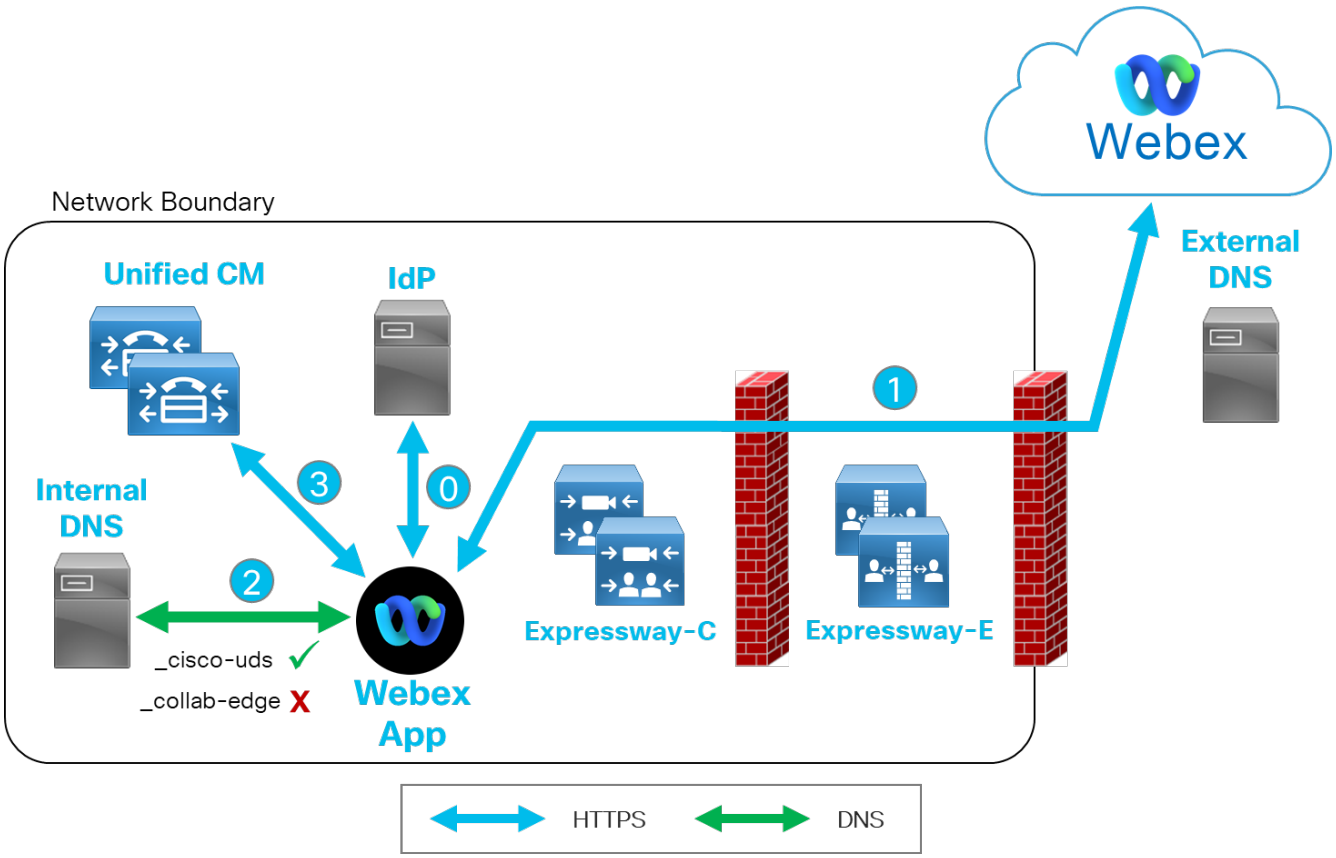
- Unified CM
- UCM Cloud
- Hosted Collaboration Solution (HCS)
- Webex Calling

Since this document is focused on migrating from Jabber to Webex, it will focus on Webex with Unified CM calling.

Unified CM Calling is enabled by checking the Calling in Webex (Unified CM) option (or the comparable toggle through the Licensing Assignment in the future). After the Webex App has connected to the Webex platform, it will next perform service discovery for Unified CM. The Webex App will discover Unified CM just as Jabber did. The application relies on DNS SRV based discovery of Unified CM when running on the corporate network or Expressway-E (MRA) when running outside the corporate network.

Figure 14 details the discovery process for the Webex App when located inside the corporate network boundary.

Figure 13. *On-Premises Webex App Service Discovery*



The flow depicted in Figure 14 is as follows:

1. As mentioned earlier, this document assumes that all services are SSO enabled (Webex and Unified CM). This means that the Webex App performed an SSO based login to Webex previously. The IdP will have presented the Webex App with a SAML cookie upon successful authentication. This SAML cookie is used to gain access to Webex services. Later in the flow, the SAML cookie will be reused for other services.

2. On the initial login screen, before authentication, the user typed in their email address, for example, *alice@example.com*. This address will be used for the Unified CM discovery process. The Webex App downloads licensing assignment from the Webex Site and determines that Unified CM calling is enabled. This will prompt the Webex App to initiate the discovery process.

3. The Webex App sends the two discovery DNS SRV queries just like Jabber does. The Webex App uses the domain name entered by the user at initial sign-in to send the DNS queries. This domain is referred to as the Voice Services Domain. The DNS queries sent to DNS are:

   - *_cisco-uds._tcp.example.com*
   - *_collab-edge._tls.example.com*

   Note: For organizations with a different Webex domain from their Voice Services Domain, or for organizations with multiple Voice Service Domains, Control Hub allows configuration of different Voice Service Domain(s), on a per user basis. This is covered in detail later in this document.

   In this example, the Webex App is running on the corporate network, so DNS will return a positive result for the *_cisco-uds* query, pointing to the FQDN of a Unified CM node in the deployment.

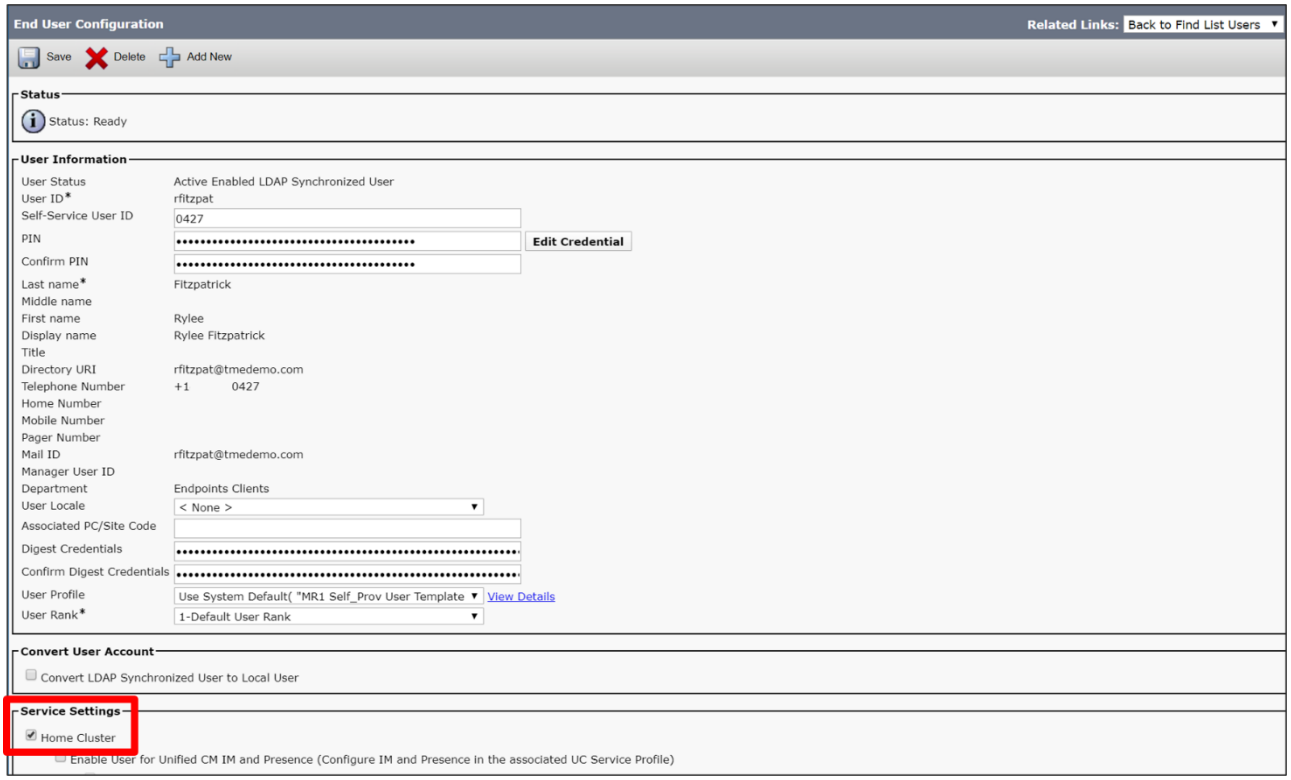
4. The Webex App connects to the Unified CM node that is returned from the DNS SRV query. The Unified CM node that the Webex App initially connects to may not be part of the Webex App users' home cluster. As such the Webex App now needs to perform home cluster discovery.

The home cluster discovery flow for the Webex App is identical to the home cluster discovery flow for Jabber described previously.

Home cluster discovery is the process whereby the Webex App makes a primary connection to any Unified CM node in the organization and is then redirected to the publisher node of the user's home cluster. The user's home cluster is the cluster where the user will obtain services for configuration download, device registration, desk phone control mode, and other services. A user's home cluster is defined administratively, by associating the user with their home cluster. Home cluster is set in bulk using the BAT tool or can be done manually on the end user configuration page.

Figure 15 shows the Home Cluster checkbox checked for an end user on this cluster.

Figure 14. *Unified CM: Home Cluster Setting*



As mentioned previously home cluster discovery relies on the Intercluster Lookup Service (ILS) and ILS should be configured between all Unified CM clusters.

Home cluster discovery for Webex as described and shown above also applies to MRA-based remote connections, whereby Expressway-C performs the home cluster discovery on behalf of the remote Webex App.

Home cluster queries sent by the Webex App are as follows:

- https://**UnifiedCM_FQDN**:8443/cucm-uds/clusterUser?username=**alice**
- https:// **UnifiedCM_FQDN**:8443/cucm-uds/clusterUser?email=**alice@example.com**

As before, the *Unified CM_FQDN* component of the above URLs is determined by the Unified CM address returned from the DNS SRV query for *_cisco-uds*.

Note: For Webex App connections over MRA, Expressway-C will perform the home cluster query against the internal DNS server.

The user identifier at the end of the query will be based on the email address the user types into the Webex App on the primary login screen. The Webex App sends two queries, one using username, and one using email. The reason for two queries is to cater for organizations who do not standardize on using username as UID in Unified CM.

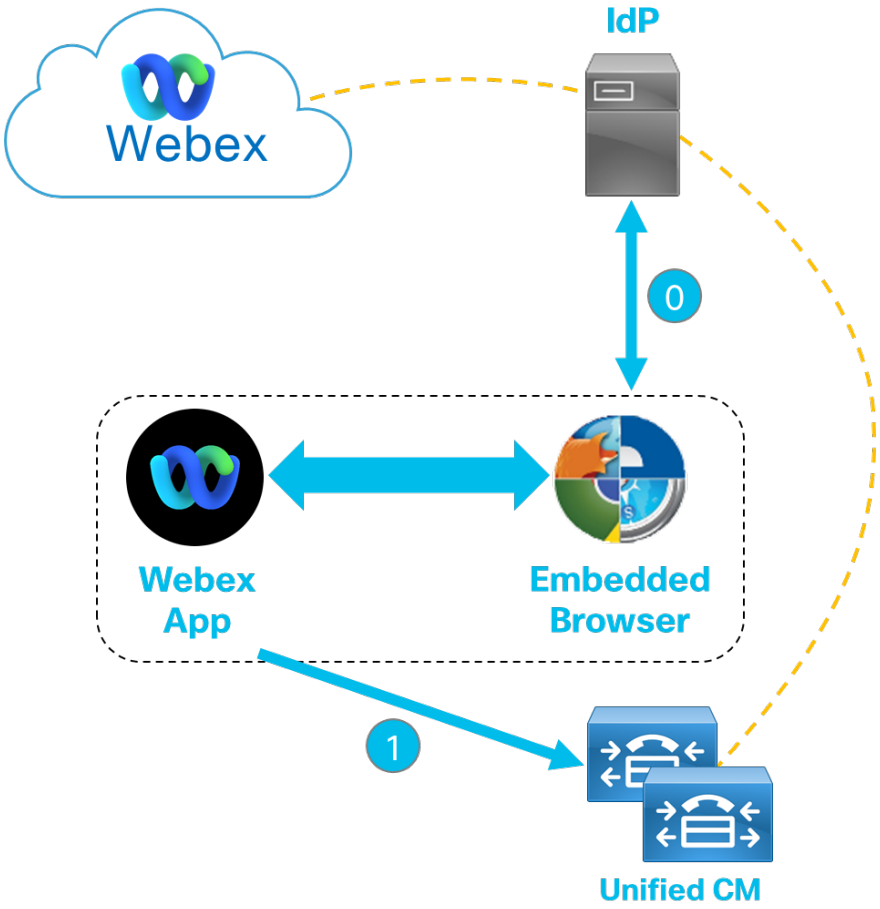
Note: With Unified CM 10.5.2 and later, users email addresses are synced from LDAP directory during LDAP sync.

As described before, once home cluster discovery is successful, the Webex App will connect to the publisher node of the home cluster to request a list of all cluster nodes, connect to a randomly selected node from the list returned, and then request the download of user configuration. Finally, the Unified CM node will challenge Webex for authentication.

The Webex App has previously authenticated via SSO when connecting to the Webex Site. Unified CM is also SSO enabled, with the same IdP as the Webex Site. As such, the Webex App reuses the existing SAML token received from the IdP to gain access to Unified CM – there is no need for the user to explicitly authenticate with Unified CM. If SSO was not enabled on the Webex Site as well as Unified CM, the user would need to manually enter username and password again, to authenticate to Unified CM.

Figure 16 shows the Webex App embedded browser authentication flow.

Figure 15. *Webex App Embedded Browser Flow with Unified CM*



The flow depicted in Figure 16 is as follows:

1. A SAML cookie have already been received from the IdP during the previous Webex service authentication.
2. The Webex App uses the existing SAML cookie to gain access to Unified CM services without the user needing to explicitly authenticate.

Once the Webex App has authenticated with Unified CM, it will retrieve an OAuth refresh token. The Webex App uses the OAuth refresh token to retrieve an OAuth access token from Unified CM. The OAuth Access Token is used to gain access to specific services including UDS. This flow assumes that OAuth Refresh Token Flow is enabled in Unified CM.

Next, the Webex App downloads configuration from Unified CM including

- Service profiles
- Jabber configuration
- End user configuration
- Device list
- Device configuration

The Service Profile will detail specific services and the service location (FQDN) that the Webex App should connect to if configured. The service profile may include some or all of the following services:

- CTI
- Jabber Client Configuration
- Voicemail

The Webex App will connect to the CTI service if the user selects to run in desk phone control mode. The end user account in Unified CM will require the role of *Standard CTI Enabled* to run the Webex App in desk phone control mode. This role may have already been enabled for Jabber.

The Webex App will download the Jabber client configuration. This configuration is available in Unified CM 12.5 and above. The configuration is equivalent to what can be configured in the jabber-config.xml file. The jabber-config.xml file is downloaded if available.

The Webex App will connect to the Unity Connection server as defined in the Service Profile. The Unity Connection service will provide voicemail capabilities to the Webex App. And if SSO is enabled on Unity Connection, the user will not have to explicitly authenticate with the service.

The Webex App will connect to a Unified CM node as defined in the CM Group list for softphone services (SIP). It will use the same device types as Jabber for softphone registration.

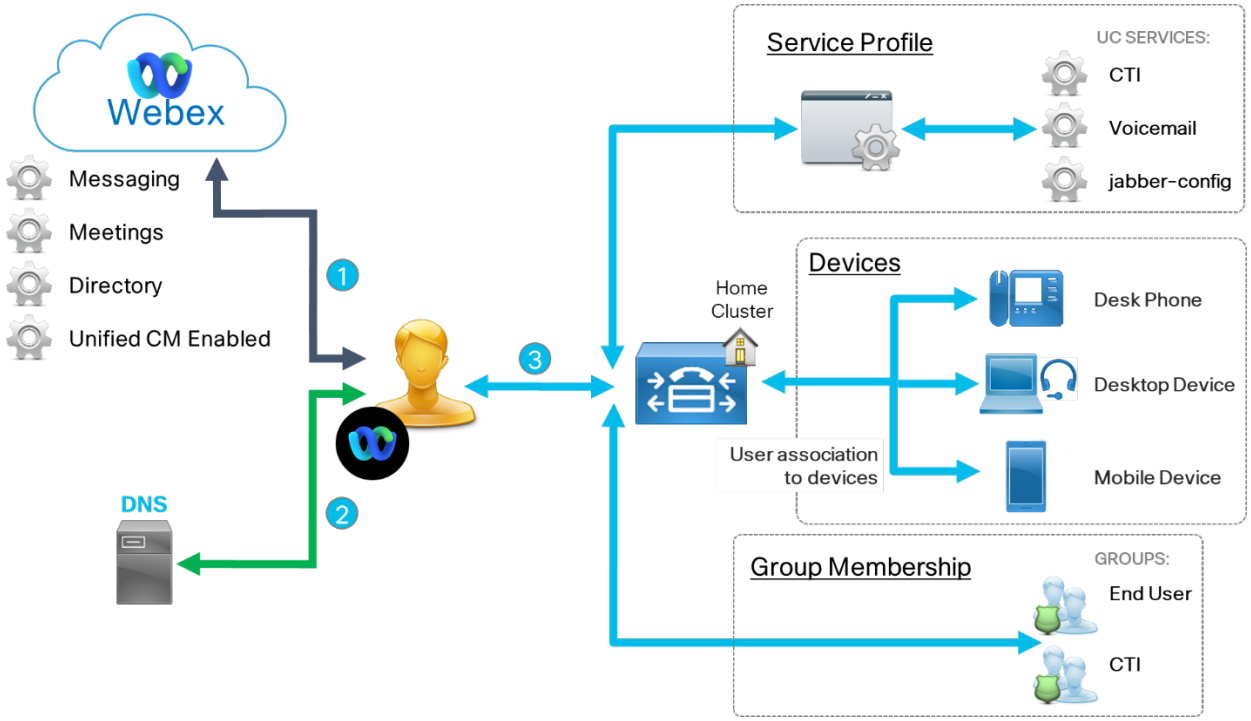
Table 4 show the device types in Unified CM based on the operating system of the Webex client application is running on.

Table 4. *Webex App Operating System Device Type*

Operating System	Unified CM Device Type	Unified CM Device Icon
Windows	Cisco Unified Client Services Framework (CSF)	
Mac	Cisco Unified Client Services Framework (CSF)	
Android Phone	Cisco Dual Mode for Android (BOT)	
iPhone	Cisco Dual Mode for iPhone (TCT)	
Android Tablet	Cisco Jabber for Tablet (TAB)	
iPad	Cisco Jabber for Tablet (TAB)	

Figure 17 summarizes service discovery for the Webex App when enabled for calling with Unified CM.

Figure 16. *Webex App with Unified CM Configuration Architecture*

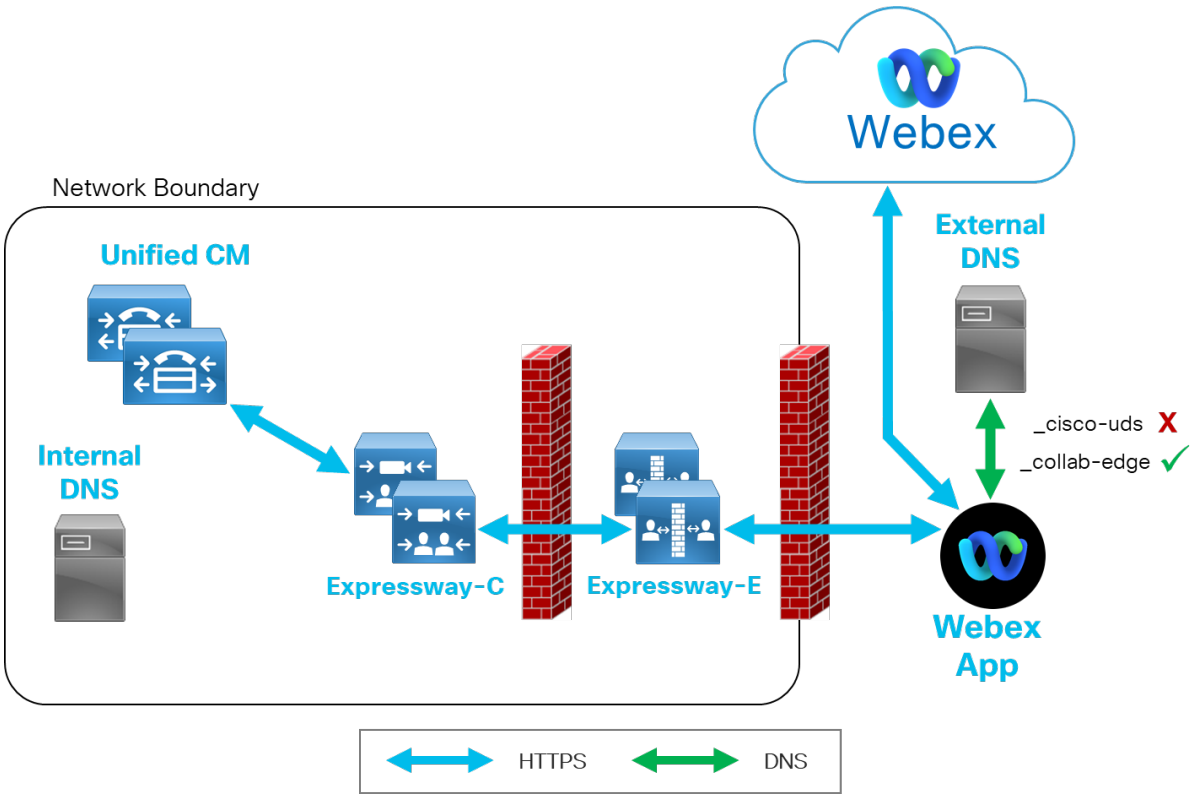


The flow depicted in Figure 17 is as follows:

1. Connect to Webex services and download calling behavior configuration detailing Unified CM enablement.
2. Begin service discovery process by sending DNS SRV queries.
3. Connect to Unified CM and download Service Profile to determine additional available services.

In the case of the Webex App outside the on-premises network boundary, the discovery depicted in Figure 17 is the same, except that the DNS SRV query is answered by external DNS resulting in the application connecting to Unified CM through Expressway MRA rather than directly. As shown in Figure 18, service discovery and service profile download are handled by Expressway-C on behalf of the Webex App.

Figure 17. *Expressway Mobile and Remote Access Webex App Service Discovery*



Subsequent Logins

The Webex App will maintain service details in a cache file that is stored on the local disk. The OAuth tokens for Webex and Unified CM services are also be stored. This information is used for subsequent logins. For example, the Webex App will use the OAuth token to gain access to other collaboration services without a requirement to authenticate each time. Another benefit of this approach is that the Webex App will connect to Unified CM services, even if connectivity to the Webex service is unavailable (for example, during an Internet outage).

Note: Cache files are encrypted before being stored on local disk.

Directory Integration

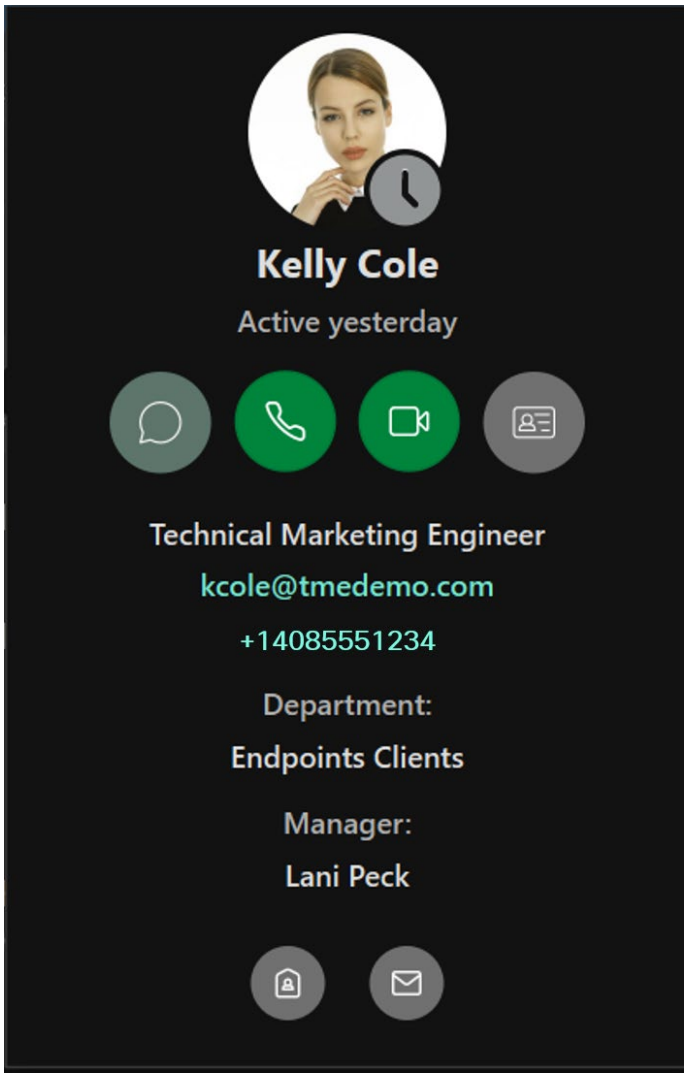
The Webex App connects to the Webex Platform for directory services. The Webex App relies on directory services for several purposes including:

- Contact Card
- Contact Search

- Contact Resolution
- Incoming Call Resolution

For example, the contact card of user kcole@tmedemo.com is shown in Figure 19.

Figure 18. *Webex App User Contact Card*



The Webex App retrieved the following information from Webex directory service to populate the contact card:

- Display Name
- Directory Photo
- Job Title

- Phone Number(s)
- Department
- Manager

Users and their associated attributes can be synchronized to Webex directory services using one of the following methods:

- Directory Connector
- SCIM
- CSV file
- People API
- Manual

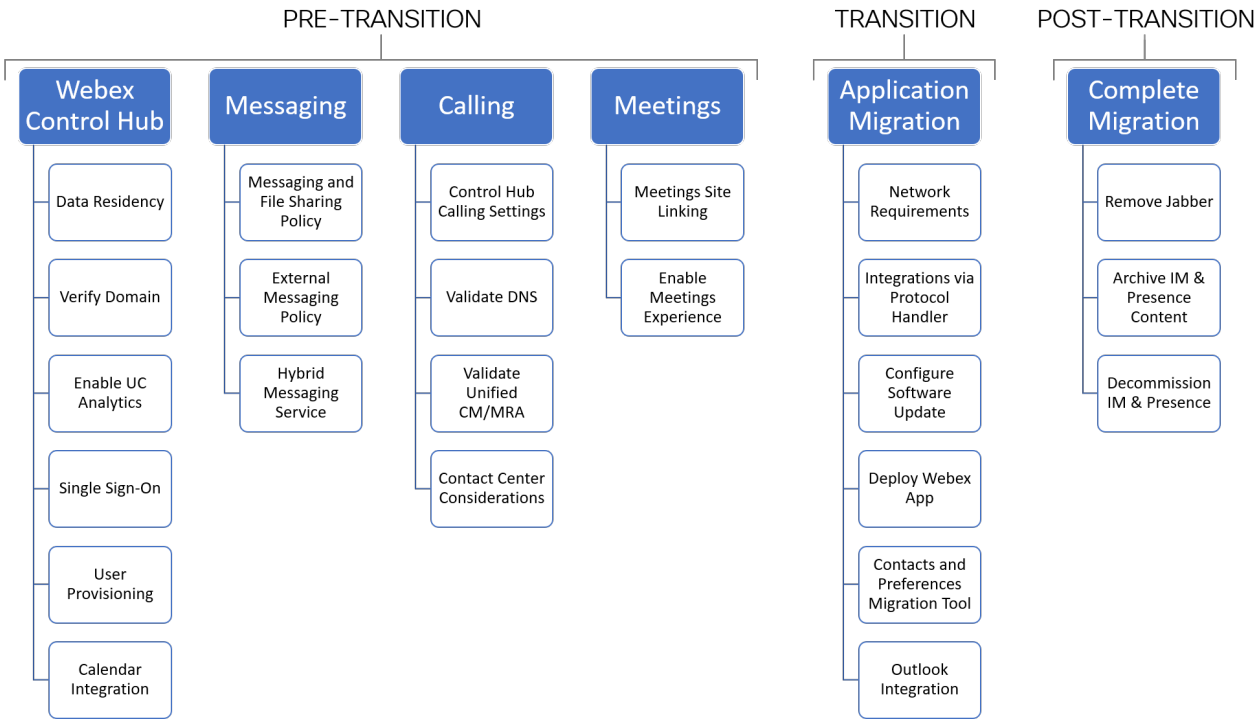
Directory Connector is the preferred method for synchronizing users to Webex. Directory Connector connects directly to Microsoft Active Directory and can synchronize user information to Webex at regular intervals. It is important to sync the entire directory to Webex, if you plan for end users to be able to search the entire directory from the Webex App. The Webex App can also search for users against the Outlook Address Book when running on a Windows PC.

Transition

Overview of this Transition Deployment Guide

This section focuses on what needs to be done to migrate from Jabber to the Webex App. Figure 20 shows the typical Jabber to Webex deployment transition

Figure 19. *Jabber to Webex Deployment Transition*



As shown in Figure 20, the transition is broken down into three high-level sets of steps to be considered for this transition:

- **Pre-transition steps** - These are the preliminary steps that should be done to prepare the environment prior to making the transition.

  The pre-transition set of steps are organized into sections to simplify the steps and allow focus on each of the collaboration workloads: messaging, calling, and meetings.

  - *Webex Control Hub* section - Focused on the basic setup for the Webex organization.

- *Messaging* section – Focused on possible messaging service configurations available in Control Hub as well as Hybrid Messaging Service which provides messaging interop between Unified CM IM&P and Webex during a migration.
- *Calling* section - Focused on the steps required to migrate Unified CM calling capabilities from Jabber to the Webex App. This section will also call out the specific calling mode of Jabber Cross Launch from the Webex App. This mode is targeted at users who need advanced Contact Center features.
- *Meetings* section – Focused on what is required to migrate meetings capabilities from the Webex Meetings App to the Webex App.

- **Transition steps** – These are the steps to implement the transition from Jabber to Webex.

  The transition set of steps involves the actual migration between the Jabber and Webex applications and covers all the necessary as well as optional steps to make this transition.

- **Post-transition steps** – These are the steps that should be done to complete the transition.

  In this case, the post-transition set of steps details how unneeded Jabber clients and collaboration services can be decommissioned.

It is worth pointing out that not all the deployment transition steps described here are mandatory and further, that the steps within a specific set of steps may be completed in a different order or at a different time.

Note: This document does not cover transitioning call control from on-premises Unified CM to cloud Webex Calling. For information about that transition refer to the Unified CM to Webex Calling transition documents available at https://www.cisco.com/go/ct.

Pre-Transition Steps and Considerations

Below are the pre-transition steps to consider when performing the client transition from Jabber to Webex.

Prior to embarking on a transition, in order to determine the feasibility and potential modifications required, it is important to consider aspects of your existing environment. Likewise, you must understand the key elements of the Webex offer in comparison with the existing on-premises deployment.

1. Setup Control Hub

Control Hub is the administrative portal for managing Webex services as well as the Webex App. Webex Control Hub is available at https://admin.webex.com/.

The following are the sub-steps involved in setting up Control Hub for the Webex App:

i. Understand Data Residency
ii. Verify Domain
iii. Enable UC Analytics
iv. Enable Single Sign-On
v. Provision Users
vi. Integrate Calendar

i. Understand Data Residency

Webex datacenters will store customer data from the Webex App. Data stored includes user identities, encryption keys, and user generated content. Organizations can choose which geo-based datacenter stores their data. The datacenter should be selected when the Webex Organization is being created.

For more information on data residency refer to the *Data Residency in Webex* article available at https://help.webex.com/en-us/oybc4fb/Data-Residency-in-Webex.

ii. Verify Domain

Once the Webex org has been acquired for your organization, you must use Control Hub to claim the domain as proof of ownership. This is a mandatory step. This process involves publishing of a DNS TXT record for your domain which Webex can resolve.

Refer to the *Manage Your Domains* article available at https://help.webex.com/en-us/nxz79m5/Add-Verify-and-Claim-Domains.

iii. Enable UC Analytics

Unified CM and Jabber analytics for your organization can be viewed in Control Hub. Unified CM analytics can be viewed in Control Hub by enabling Webex Cloud Connected UC. Jabber analytics can be viewed in Control Hub by

enabling Jabber Telemetry with Org ID. This is not a mandatory step for migration to the Webex App, however it is recommended for the following reasons:

- To provide visibility into the existing Unified CM and Jabber deployment pre-migration.
- To provide visibility into migration progress at migration time.
- To take advantage of future Cloud Connected UC (CCUC) operational features.

CCUC allows organizations to view Unified CM analytics in Control Hub. This is achieved by installing the CCUC plugin on existing Unified CM clusters. The plugin provides for Unified CM connectivity to Webex, which enables publishing of Unified CM analytics to Control Hub.

For more details on the benefits of CCUC refer to the *Cisco Webex Cloud-Connected UC Data Sheet* available at https://www.cisco.com/c/en/us/products/collateral/unified-communications/webex-cloud-connected-uc/datasheet-c78-743868.html.

Jabber can post usage telemetry to the Webex analytics service and organizations can view their own Jabber telemetry in Control Hub. The data collected by Jabber does not contain any Personal Identifiable Information (PII) – that is, individual users cannot be identified from the data that is sent to the Webex service. Control Hub allows organizations to view several Jabber data points including:

- Breakdown of platform Jabber is running on
- Breakdown of versions of Jabber
- Number of video/audio calls
- Call quality
- Number of chats
- Mobile Remote Access (MRA) usage

To view your organization's Jabber telemetry in Control Hub, your organization's telemetry data needs to be marked with your Webex Organization ID. The Webex Organization ID is a 32-character string which identifies the Webex organization. The Webex Organization ID can be obtained by logging into Control Hub and clicking Account.

The keys shown in Figure 21 should be added to the jabber-config.xml file (or to the Jabber Client Configuration UC Service if running Unified CM 12.5). Replace *customer_ID* with your Webex Organization ID.

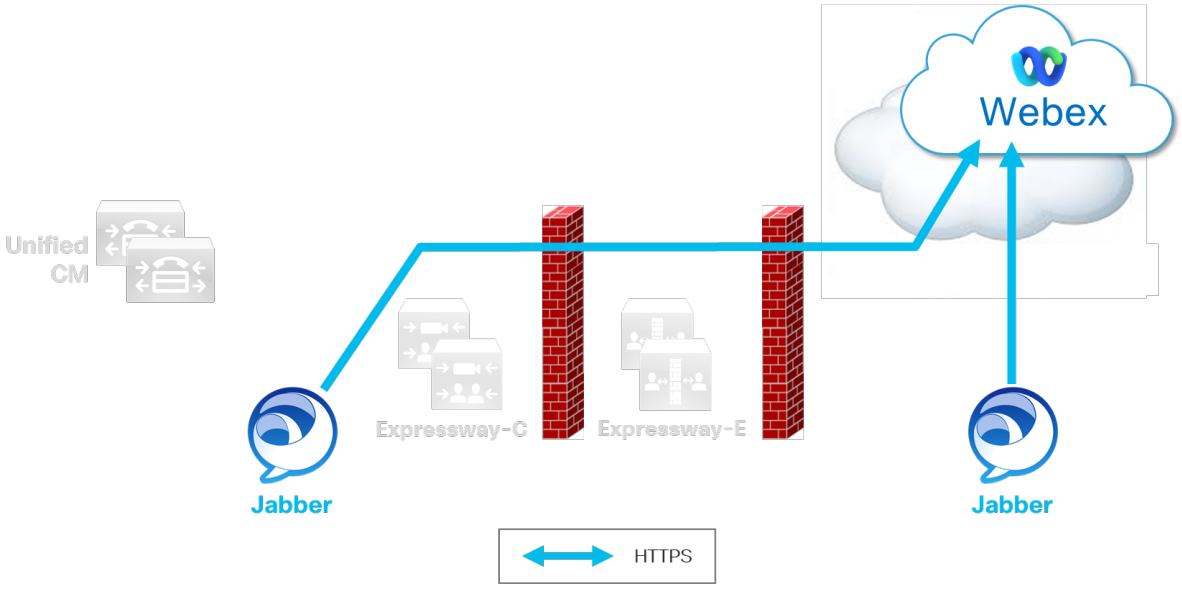
Figure 20. *Jabber-config to Enable Telemetry in Webex Control Hub*

```
<TelemetryEnabled>True</TelemetryEnabled>
<TelemetryEnabledOverCellularData>True</TelemetryEnabledOverCellularData>
<TelemetryCustomerID>customer_ID</TelemetryCustomerID>
```

Note: Users can disable Jabber telemetry from the Jabber client help menu, even if the administrator has enabled in the jabber-config.xml file.

Jabber will post the telemetry data to Webex at regular intervals (see Figure 22).

Figure 21. *Jabber Telemetry Flow*



Ensure Jabber clients can reach the Webex analytics service. The following may need to be configured on your firewall: *Outbound TCP 443 metrics-a.wbx2.com/metrics/api/v1/metrics*.

As shown in Figure 22, telemetry is posted to Webex via HTTPS. Jabber will validate the certificate presented by the Webex analytics service. The following certificate should be installed on the local device to prevent certificate validation from failing: *GoDaddy Class 2 Certification Authority Root Certificate*.

The Jabber analytics dashboard will appear automatically in Control Hub 24 hours after the first Jabber telemetry packet is received, and marked with your Webex Organization ID. The Jabber analytics dashboard can be viewed in the Analytics tab.

iv. Enable Single Sign-On (SSO)

While SSO is not a mandatory requirement for migration to the Webex App, it is highly recommended. The Webex App may sign-in to several different services including Webex, Unified CM, Unity Connection, and other services. By enabling SSO across all services, users can have a single login experience for all services. SSO also provides security benefits including support for multiple types of authentication, for example, certificates or MFA.

SSO can be enabled for the Webex organization on Control Hub. Control Hub supports SSO integration with any IdP that supports the SAML standard.

For more information on enabling SSO for your Webex organization refer to the *Single Sign-On Integration in Control Hub* article available at https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Control-Hub.

If SSO is not enabled for the Webex organization, Webex users will sign in using a user ID and password. These passwords will be maintained by Webex, and they will not be coupled or synchronized with corporate directory passwords. If a user changes their corporate directory password, this will not change their Webex App password. The user will also need to manually sign into other services (for example, Unified CM for calling).

If Webex SSO is not enabled, users will receive an automated welcome email once their account is created in Control Hub. This email will provide a link for users to set their Webex password. Refer to the Provision Users section below for more details.

v. Provision Users

Before users are added to Control Hub, License Assignment Templates should be configured. The License Assignment Template will allow for automatic licensing of users for services once they are synced to Control Hub. As shown in

Figure 22. *Webex Control Hub: License Assignment*

For more details on configuring License Assignment Templates refer to the *Set Up Automatic License Assignment Templates in Cisco Webex Control Hub* article available at https://help.webex.com/en-us/n3ijtao/Set-Up-Automatic-License-Assignment-Templates-in-Cisco-Webex-Control-Hub.

Users must be created in Control Hub before they can use the Webex App. As shown in Table 5, Control Hub provides several methods for provisioning user accounts.

Table 5. *Webex Control Hub User Provisioning Methods*

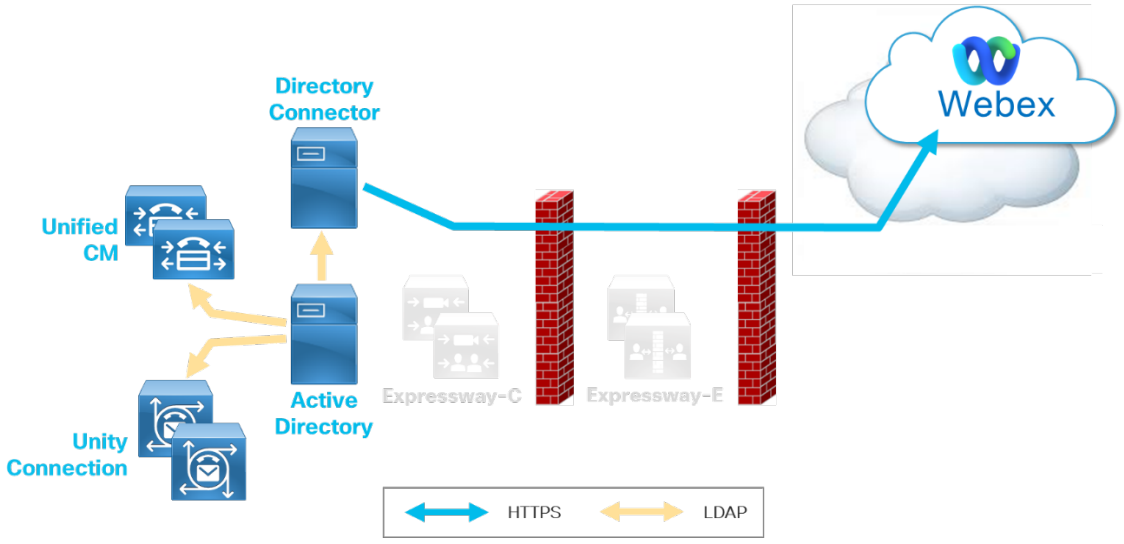
User Provisioning Service	Details
Directory Connector	Director Connector manages user syncing from Active Directory (AD) to Webex. It also allows AD groups to be synced to Webex, which allows some user services to be enabled based on AD groups.

System for Cross-Domain Identity Management (SCIM)	System for Cross-Domain Identity Management or SCIM is an open standard for managing user identities across different cloud services. Users can be synced to Webex from services including Azure and Okta via SCIM.
CSV File	Webex Control Hub allows for user provisioning via a CSV file. The CSV file can be used to add user accounts as well as configuring user services.
Manual	User accounts can be managed directly in Webex Control Hub.

Directory Connector is the recommended tool for user provisioning. Existing Jabber deployments, will likely already synchronize users from Active Directory to Unified CM.

Figure 24 details the architecture for user provisioning via Directory Connector.

Figure 23. *Webex Directory Connector Architecture with Unified CM LDAP Synchronization*



As shown in Figure 24, LDAP synchronization can be enabled on Unified CM and Unity Connection to synchronize users directly from AD. In turn, Directory Connector can be deployed to synchronize users from Active Directory into Webex.

Director Connector is an application that is installed on a machine running the Windows Server operating system.

For more details on deploying Webex Directory Connector, refer to the *Deployment Guide for Cisco Directory Connector* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/directoryconnector/cmgt_b_directory-connector-guide-admins.html.

If AD is not available for your organization, another of the following user provisioning methods can be used:

- For more details on provisioning users in Webex from Azure AD, refer to the *Synchronize Azure Active Directory Users into Control Hub* article available at https://help.webex.com/en-us/6ta3gz/Synchronize-Azure-Active-Directory-Users-into-Control-Hub.
- For more details on provisioning users in Webex from Okta, refer to the *Synchronize Okta Users into Cisco Webex Control Hub* article available at

https://help.webex.com/en-us/nmm9pzdb/Synchronize-Okta-Users-into-Cisco-Webex-Control-Hub.

- For more details on provisioning users in Webex via CSV files, refer to the *Add Multiple Users in Cisco Webex Control Hub with the CSV Template* article available at https://help.webex.com/en-us/nlkiw8e/Add-Multiple-Users-in-Cisco-Webex-Control-Hub-with-the-CSV-Template.

Note: If Directory Connector is enabled for the Webex Organization, users can only be added or removed based on AD adds/removes. User configurations can be updated via another means while Directory Connector is enabled. e.g., Users can be added to Webex via Directory Connector and their configurations may be updated via CSV file.

Note: Once users are added to Control Hub, they will receive an automated email welcoming them to their Webex account with a link to get started. This email can be deactivated if users should not receive this email. SSO must be enabled for the Webex Organization to deactivate this welcome email.

For more details on suppressing the automated welcome email refer to the *Suppress Automated Emails* article available at https://help.webex.com/en-us/nqj88gt/Suppress-Automated-Emails.

Note: The Webex Common Identity (CI) service provides directory services to the Webex App. For example, when a user performs a contact search in the Webex App, the search will be performed against CI. The Webex App will not search directly against LDAP Directory or Unified CM UDS services. For this reason, it is very important to sync **all** users in the organization to Webex, if all users should be searchable from the Webex App. It is also important to ensure relevant phone numbers are synchronized to Control Hub, to successfully deploy Unified CM calling with the Webex App.

vi. Integrate Calendar

Calendar integration is an important part of a successful migration to the Webex App. Webex calendar integration is known as Hybrid Calendar Service. This integration is not mandatory but highly recommended to enable calendar services within the Webex App.

Hybrid Calendar Service enables the following in the Webex App:

- Ability to view calendar from the Webex App.
- Easy meeting scheduling from the Webex App.
- One Button to Push (OBTP) meeting join experience.

Hybrid Calendar also enables calendar integration for personal and room video systems deployed in the organization.

Hybrid Calendar Service supports the following calendar services

- Office 365
- Google Calendar
- Microsoft Exchange (on-premises)

Since Office 365 and Google are cloud-based calendar sources, Webex allows for a cloud-to-cloud integration (that is, no on-premises infrastructure setup is required). Enabling Webex Hybrid Calendar Service with Microsoft Exchange (on- premises) requires deployment of Expressway nodes running the Hybrid Calendar Service.

For more details on deploying Webex Hybrid Calendar Service refer to the *Deployment Guide for Cisco Webex Hybrid Calendar Service* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/calendarservice/cmgt_b_deploy-spark-hybrid-calendar-service.html.

Note: If Hybrid Calendar Service is not deployed for the organization, calendar and scheduling services within the Webex App will be limited. Users will not have a consistent view of their calendar within the Webex App across desktop and mobile. Meeting scheduling will also have limited functionality.

2. Messaging: Understand messaging options

This step focuses on the migration of the messaging service. Jabber messaging service is provided by on-premises Unified CM IM&P server nodes. Webex App messaging is provided by the Webex platform.

The following are the sub-steps involved in preparing for Webex messaging with the Webex App:

i. Understand Messaging and File Sharing Policy
ii. Consider External Messaging Policy
iii. Enable Hybrid Messaging Service

i. Understand Messaging and File Sharing Policy

Note: All messaging and file sharing policy with Webex messaging is managed using Webex Control Hub.

Message Retention

Webex messaging is persistent. This means that messages and files sent using the Webex App are written to storage in a Webex Datacenter and will be available within 1:1 and groups spaces within the Webex App for a defined period. This period is known as the retention period.

The Control Hub administrator defines the retention period for all Webex App users within the organization. The retention period defaults to 'Indefinitely' meaning messages will never be deleted and will always be available within the Webex App. The retention period can be set to a defined period in units of months. The shortest allowed retention period that can be set in Control Hub is one month; however, this can be set to be less than one month on request to Cisco.

Messages and files will be deleted from Webex once the retention period has expired. For example, let's assume an organization has specified a retention period of one year. If a user sends a message on January 1, 2021, that message would be deleted from Webex on January 1, 2022.

Note: Message deletion at the end of a retention period is permanent. Messages cannot be retrieved once they are deleted.

It is recommended that the retention period be set for as long as possible but in accordance with any specific retention policies an organization may have. One of the benefits of Webex messaging is the fact that messages and files are persistent. Setting a short retention period will diminish this benefit and will result in a less than ideal user experience.

For specific instructions on setting the Webex Organization retention policy refer to the *Set the Retention Policy for Your Organization* article available at https://help.webex.com/en-us/nqmr56k/Set-the-Retention-Policy-for-Your-Organization.

Messaging Compliance and Data Loss Prevention

Messaging compliance and Data Loss Prevention (DLP) is a broad topic. This section refers specifically to replicating a similar messaging compliance policy with the Webex App and Webex messaging that was available with Jabber and Unified CM IM&P.

Unified CM IM&P supports several compliance methods including:

- Message logging
- Message policy management
- Ethical walls

Unified CM IM&P supports the above compliance methods via integration with third-party compliance engines.

Webex messaging supports similar integrations with Cisco and third-party Cloud Access Security Brokers (CASB) like Cisco Cloudlock, Actiance, and Verba. These integrations allow organizations to enable compliance policies such as:

- Messaging and files policy violation management
- Message archival
- eDiscovery
- Legal hold
- Ethical walls
- Space classification

Some compliance services will require that the role of Compliance Officer exists for the Webex Organization. This role can be enabled for a user by a Control Hub administrator.

For more information on integrating Webex with your compliance and DLP solution, refer to the *Control Hub (Compliance) Data Sheet* available at

https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740772.html.

Webex also offers some native messaging policy management tools. Webex Organization administrators can set the following restrictions in Control Hub:

- Restrict file sharing to your network only
- Block file preview per platform
- Block file sharing per platform
- Disable GIPHY integration
- Disable link preview

ii. Consider External Messaging Policy

By default, Webex allows for native external messaging such that Webex App users in Webex Organization example.com can message Webex App users from other Webex Organizations.

External messaging can be restricted by the administrator in Control Hub in one of the following ways:

- Block external messaging
- Restrict external messaging to administrator specified allow list

The administrator can add domains to the allow list directly in Control Hub.

For more details on restricting external messaging, refer to the *Block External Users in Webex Spaces for Your Organization* article available at https://help.webex.com/en-us/agrt8/Block-External-Users-in-Webex-Spaces-for-Your-Organization.

In addition to native external messaging, Webex allows organizations to configure the following external messaging solutions:

- XMPP Federation
- SIP Federation

Jabber with Unified CM IM&P supports both interdomain XMPP and SIP federation. Organizations that migrate to the Webex App can maintain these federations with the Webex App and Webex messaging.

Note: Only interdomain federation is supported. Specifically, the Webex Organization must have a different domain name than the federated SIP or XMPP service.

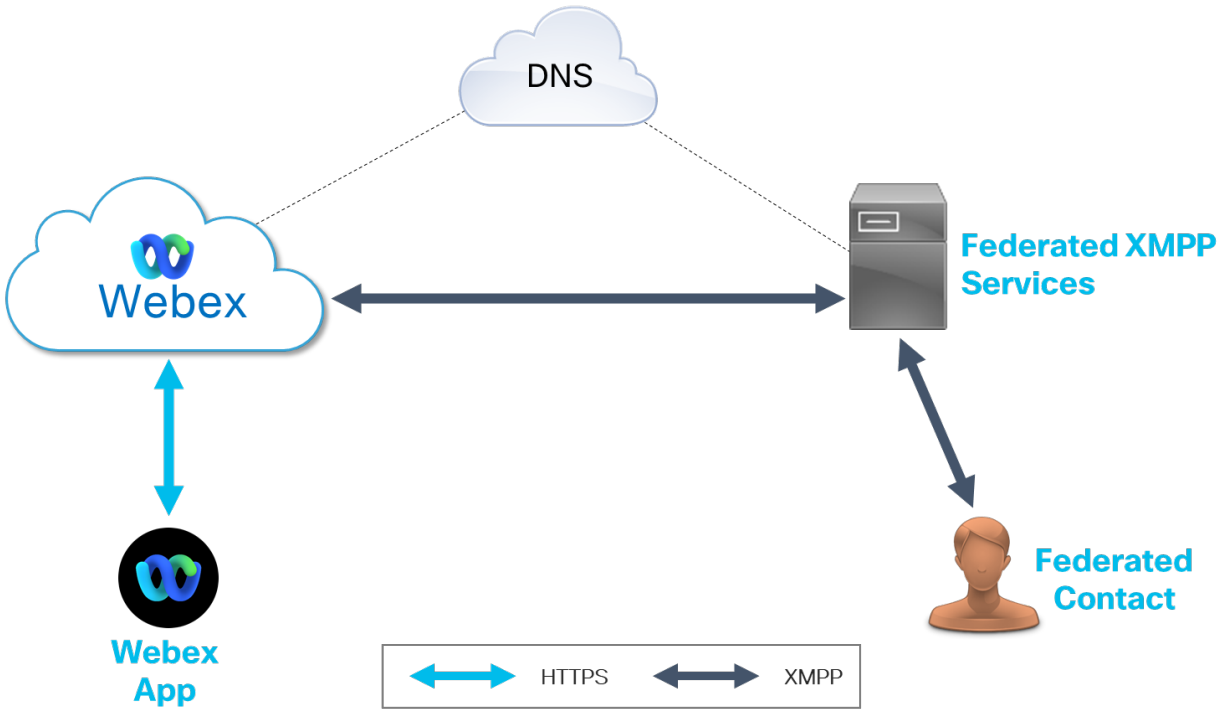
XMPP Federation

Webex XMPP federation offers support for 1:1 messaging between users using the Webex App and users using an XMPP messaging service (for example, Jabber with Unified CM IM&P).

Webex XMPP federation also offers support for 1:1 messaging between users using the Webex App and users using a SIP messaging service (for example, Skype for Business).

Figure 25 details the architecture for Webex XMPP federation.

Figure 24. *Webex XMPP Federation Architecture*



Webex will advertise XMPP capabilities via a public DNS SRV record: *xmpp-server._tcp.domain.com*. Likewise, Webex will discover third party XMPP services via their public DNS SRV record.

If XMPP federation is currently configured for Jabber, the xmpp-server DNS SRV record will need to be updated to point to Webex messaging service instead of Unified CM IM&P/Expressway. This change should be made when the organization is ready to migrate XMPP federation capabilities from Jabber to the Webex App.

XMPP federation can be enabled for a single domain per Webex organization. If there are multiple presence domains configured for the existing Unified CM IM&P deployment (flexible JID with multiple email domains), consider consolidating to a single domain prior to moving to Webex XMPP federation.

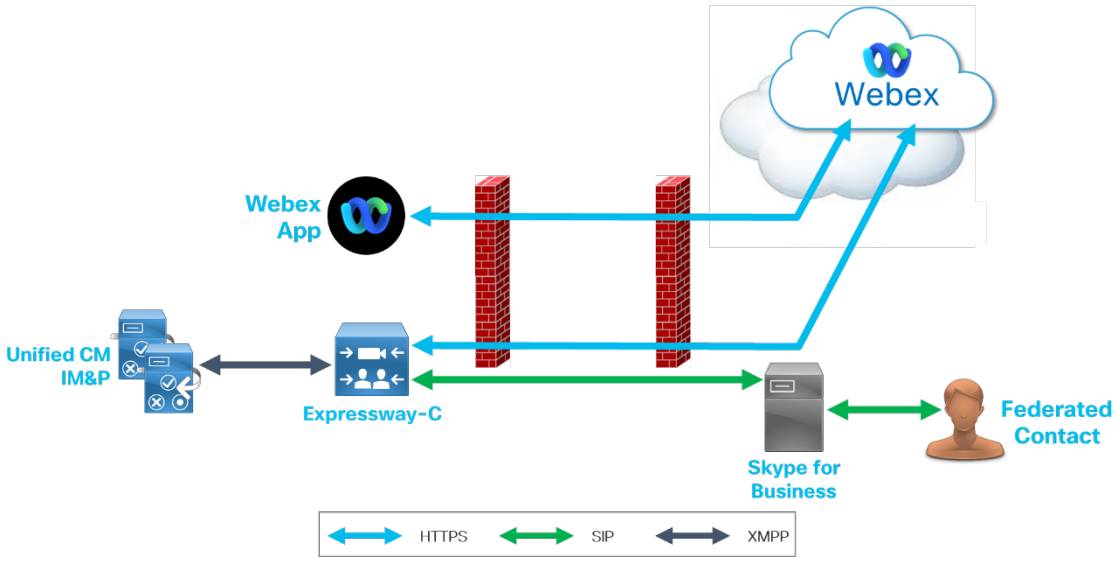
The Allow List configured for Webex external messaging also applies to XMPP federation. Therefore, restricting external messaging to specific domains will not only restrict Webex native messaging, but it will also restrict XMPP federation.

For more details on configuring XMPP federation for Webex, refer to the *XMPP Federation for Webex* article available at https://help.webex.com/en-us/05i99o/XMPP-Federation-for-Webex.

SIP Federation

Figure 26 details the architecture for Webex SIP federation.

Figure 25. *Webex SIP Federation Architecture*



Webex SIP federation is based on utilizing existing Unified CM IM&P/Expressway SIP federation to Skype for Business in conjunction with Hybrid Messaging

Service. Hybrid Messaging Services allows for messaging interop between Webex, and Unified CM IM&P via Expressway-C. Hybrid Messaging Service will be discussed in the next sub-step.

SIP federation is enabled in Control Hub for the Webex Organization. Messages are routed from the Webex messaging service to Expressway-C (Hybrid Messaging Service), and then onto Unified CM IM&P. Assuming Unified CM IM&P is already enabled for SIP federation, it routes the message to the SIP broker service on Expressway-C. Expressway-C in turn routes the message onto Skype for Business.

Note: Skype for Business domain must be different from the Webex Organization and Unified IM&P domains.

Expressway-C provides Hybrid Messaging and SIP broker services for this federation. Both services can run on the same Expressway-C node, or they can be split between different nodes.

Enabling SIP federation in Control Hub will not affect existing Jabber and Unified CM IM&P SIP federation.

For more details on enabling SIP federation for the Webex App refer to the *SIP or XMPP Interdomain Federation for Webex* article available at https://help.webex.com/en-us/n8gtpu7/SIP-or-XMPP-Interdomain-Federation-for-Webex.

Additional Considerations

The following are important messaging considerations that will not be covered in detail in this document since they are not transition impacting:

- Enterprise Content Management (ECM) provides integration between Webex and existing Content Management solutions such as SharePoint Online, Outlook, Google Drive, and Box. Users can share files stored on the organizations content management solution direct from the Webex App.

  See Enterprise Content Management For more information on ECM with Webex refer to the *Enterprise Content Management in Cisco Webex Control Hub* article available at https://help.webex.com/en-us/nuvy9lb/Enterprise-Content-Management-in-Cisco-Webex-Control-Hub.

- The Webex App supports end-to-end encryption of messages. This means that the Webex App will first encrypt a message using a key and then will send the message to the Webex service. The Webex messaging service stores the encrypted message. Message recipients will download the encrypted messages from Webex and use the encryption key to decrypt the message. The key used to encrypt/decrypt message content is retrieved from a key management service provide by the Webex platform.

  Optionally, organizations can host their own key management service. This is known as Hybrid Data Security. For more details on Hybrid Data Security, refer to the *Deployment Guide for Cisco Webex Hybrid Data Security* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/datasecurity/cmgt_b_hybrid-data-security.html.

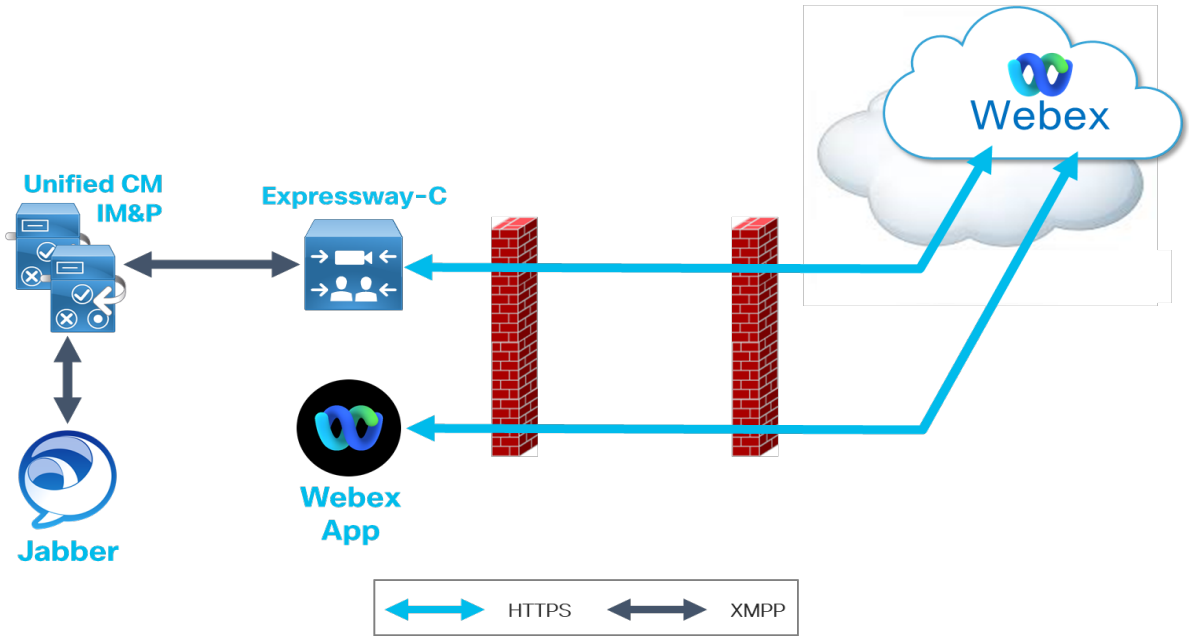
iii. Enable Hybrid Messaging Service

Hybrid Messaging Service is a solution that allows Webex App users to send and receive messages with Jabber users connected to Unified CM IM&P. Hybrid Messaging is an optional step in transitioning from Jabber to the Webex App. Hybrid Messaging should be deployed if users will be migrated from Jabber to the Webex App in groups over a period. During the migration period, Hybrid Messaging will ensure messaging between Jabber and Webex App users will be available.

Hybrid Messaging Service supports 1:1 messaging between Jabber and Webex App users. There is limited support for presence and file transfer across Hybrid Messaging Service is not supported.

Hybrid Messaging Service runs as a connector service on Cisco Expressway. Figure 27 below details the high-level architecture for Hybrid Messaging Service.

Figure 26. *Hybrid Messaging Architecture*



The Hybrid Messaging Service runs as a connector on Expressway-C, providing a bridge between Unified CM IM&P and Webex messaging. As a best practice deploy Hybrid Messaging enabled Expressway clusters at a 1:1 ratio with Unified CM IM&P clusters. For organizations who have many Unified CM IM&P clusters, consider transitioning to Centralized Unified CM IM&P before deploying Hybrid Messaging Service. For more information on transitioning between distributed multi-cluster Unified CM IM&P and centralized Unified CM IM&P refer to the *Transitioning to Centralized IM and Presence Service (IM&P) Deployment Guide* available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/mcp/DEPLOYMENT_MESSAGING-UnifiedCM_IMP_Distributed_to_Centralized.pdf.

Unified CM IM&P uses the Jabber ID (JID) to route messages to users and systems. Webex messaging service uses email address to route messages to users and systems. JID and email address do not need to match to deploy Hybrid Messaging Service. If Unified CM IM&P is not enabled for Flexible JID mode, the JID will be formed as *userID@xmppdomain*. This may differ from the user's email address. Unified CM syncs the email address attribute from the corporate directory during LDAP synchronization and maps this attribute to the Directory URI field. Unified CM IM&P then synchronizes this information from Unified CM. A user will have both a JID and a Directory URI, these may be different values. Hybrid Messaging Service running on Expressway will sync the JID and Directory URI from Unified CM IM&P at regular intervals. Hybrid Messaging Service will maintain the JID to Directory URI (Directory URI = email

address) mapping to route messages from Jabber users (JID) to Webex App users (email). Ensure Unified CM Directory URI attribute maps to the email address that is used to create the users Webex App account.

Users must be enabled for both Unified CM IM&P and Webex messaging to be enabled for Hybrid Messaging. As groups of users are migrated to the Webex App, they should be enabled for Hybrid Messaging. Users are enabled for Hybrid Messaging in the following ways:

- Manually via Control Hub
- Licensing Template
- CSV file

The CSV file method provides the most flexibility for enabling users for Hybrid Messaging in bulk as it involves changing users licensing template. CSV file method can be used to update user configuration even if Directory Connector is enabled.

As more groups of users are migrated to the Webex App, the CSV file method can be used to enable those users for Hybrid Messaging Service.
When all users have been migrated from Jabber to the Webex App, Hybrid Messaging Service can be decommissioned (unless Webex messaging SIP federation is deployed).

3. Calling: Prepare Unified CM on-premises calling for Webex

This set of steps focuses on the migration of the calling service from Jabber to the Webex App. Webex App can connect to different calling services including:

- Unified CM (on-premises)
- UCM Cloud
- Hosted Collaboration Solution (HCS)
- Webex Calling

This guide focuses on the transition from Jabber with Unified CM (on-premises) to the Webex App while maintaining Unified CM calling (hybrid).

The following steps need to be taken when undertaking the calling workload transition:

i. Webex Control Hub Calling Settings

ii. Validate DNS

iii. Validate Unified CM and Expressway Settings

iv. Contact Center Considerations

i. Webex Control Hub Calling Settings

The following settings in Control Hub should be considered when enabling Webex App users for Unified CM calling:

- Ensure Phone Number Syncing
- Licensing Assignment
- UC Manager Profiles
- Client Calling Settings

Ensure Phone Number Syncing

Phone numbers must be synced to Control Hub to successfully deploy the Webex App with Unified CM calling. This should have been completed when provisioning users the first time.

UC Manager Profiles

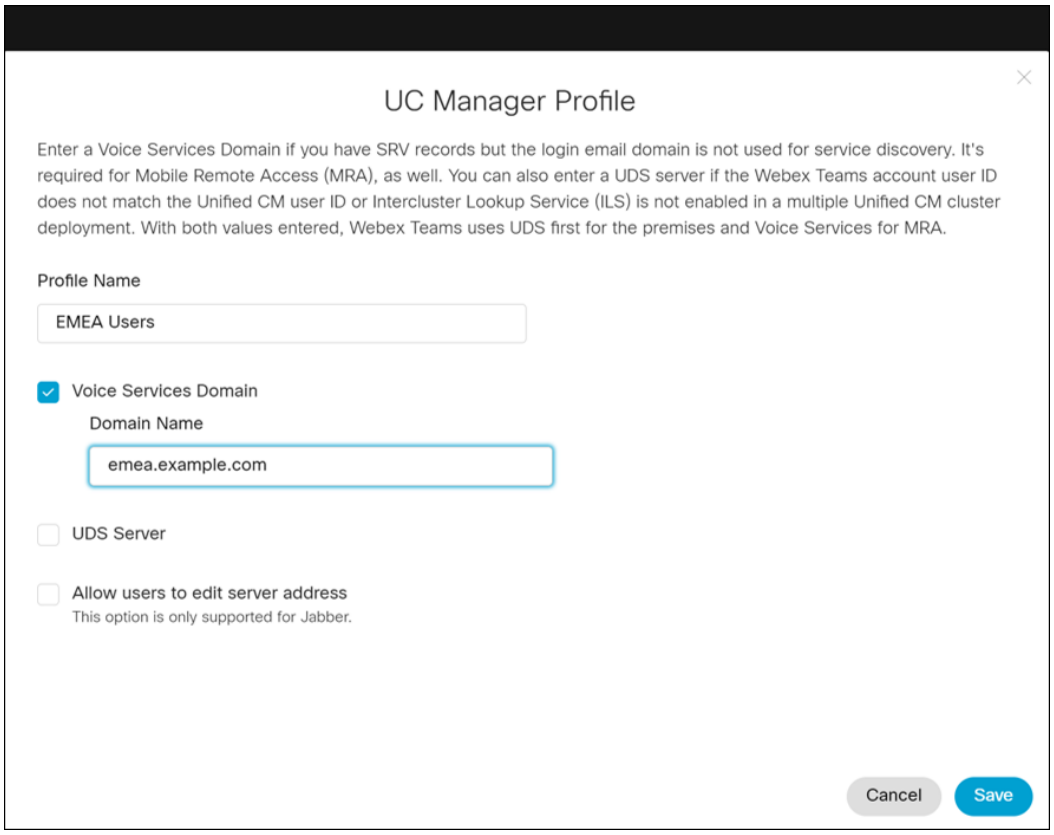
When the Webex App starts up, it will download the Unified CM enablement from Webex Control Hub and begin service discovery. The Webex App will send DNS SRV queries to discover Unified CM or Expressway-E (MRA). The domain used by the Webex App when sending the DNS SRV queries will be the domain the user used to sign in to the Webex App (the Webex Organization domain). The domain used to discover Unified CM/MRA is referred to as the Voice Services Domain.

For organizations who want to use a different Voice Services Domain, or for organizations who want to use multiple Voice Services Domains, this can be configured using Webex Control Hub UC Manager Profiles.

In Control Hub, configure a UC Manager Profile for every Voice Services Domain in your organization. The UC Manager Profile can be assigned in bulk to users using the CSV file user provisioning method. Export the CSV file from Control Hub, modify the UC Manager Profile column as needed, and import the CSV file back into Control Hub.

Figure 29 shows a UC Manager Profile with Voice Services Domain set. In this example the users sign into the Webex App with *user@example.com*. This organization has Voice Services Domains per region. This UC Manager Profile is enabled for all EMEA based users. These users' Webex App will perform Unified CM/MRA discovery using *emea.example.com.*

Figure 27. *Webex Control Hub: Voice Services Domain*

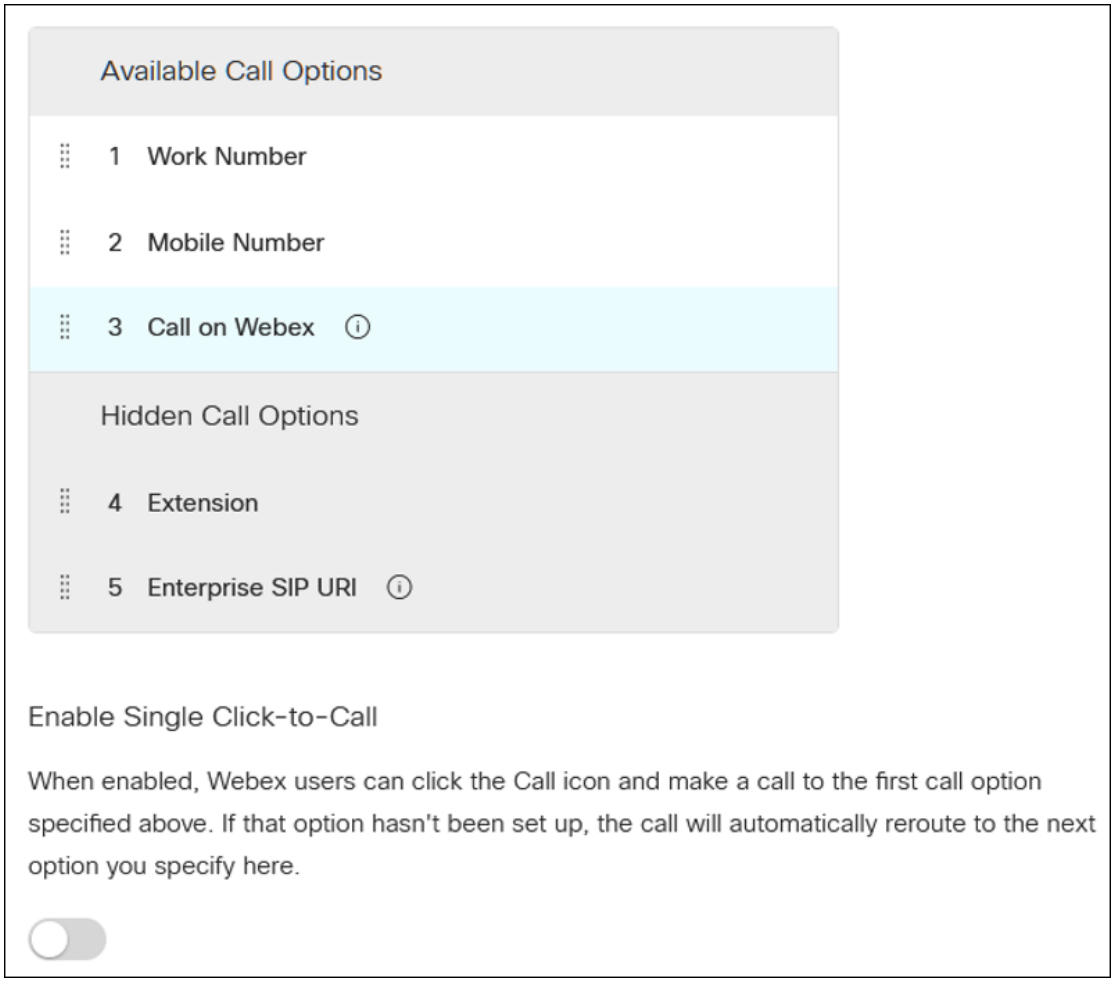


Client Calling Settings

There are several Webex App calling experience settings that can be configured in Control Hub.

Figure 30 details the Call Settings option. Call Settings define what happens when a Webex user clicks the Audio Call or Video Call buttons in a 1:1 space, contact card, or from the search bar. The options set under *Available Call Options* will be displayed in a drop-down menu. The options shown under *Hidden Call Options* will not be displayed. The user can then select the appropriate available calling option to place the call.

Figure 28. *Webex Control Hub: Call Settings for Webex with Unified CM*



The calling options shown in Figure 30 can be set under **Calling > Client Settings**

Note: Changes made to Client Settings will apply to all Webex App users in the organization.

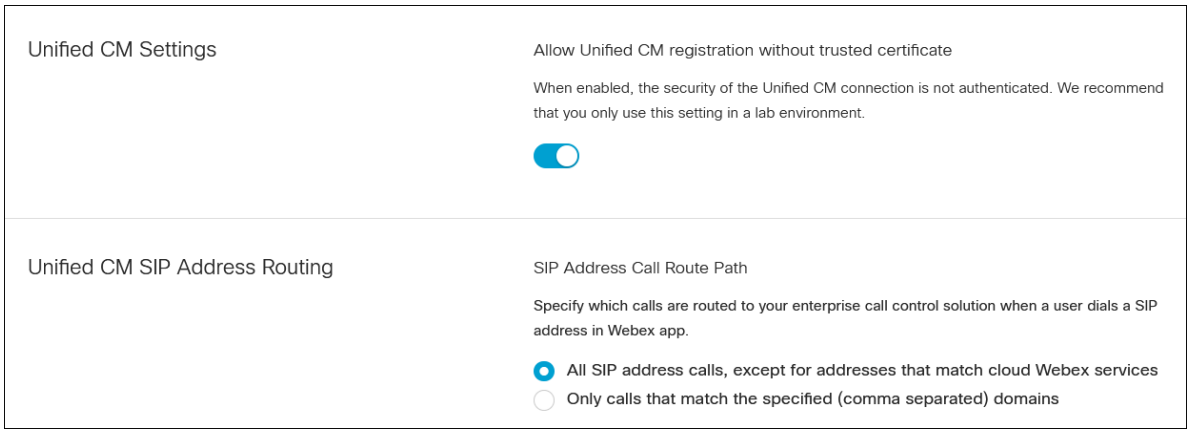
"Call on Webex" refers to the native calling service available when using the Webex App. If a user selects this option, the call will not be routed via Unified CM, it will be routed via the native Webex calling service. If you do not want users to have native Webex calling capabilities for 1:1 call, this option should be moved down to the Hidden Call Options section.

Note: Users will still be able be able to make native Webex calls to spaces and will still be able to receive incoming native Webex calls even when "Call on Webex" is hidden.

By toggling “Enable Single Click-to-Call” users will not be presented with the drop down to select calling option. The Webex App will simply call the first available option under *Available Call Options*.

As shown in Figure 31, additional Control Hub Client Setting configuration options include Unified CM settings and SIP address routing

Figure 29. *Webex Control Hub: Unified CM Settings and SIP Address Routing*



When enabling the Unified CM Settings toggle, the Webex App will ignore invalid certificates presented by Unified CM server nodes. The Webex App will continue with Unified CM connection even if the certificate presented is invalid. The best practice recommendation is to only enable this toggle for trial organizations or while performing lab testing.

Note: If this toggle is not set, the Webex App will discontinue connection to Unified CM if presented with an invalid Tomcat certificate. Unlike with Jabber, the user will not be prompted to accept an invalid server certificate.

The Unified CM SIP Address Routing option allow the administration to set the Webex App behavior when a user places a call to a SIP URI. The Webex App will always make a native Webex calling service call when a user dials a SIP URI ending with **.webex.com* – for example, a user makes a call to alice@example.webex.com. This call will not be routed via Unified CM, it will be made by the native Webex calling service.

By default, SIP URI calls to all other domains will be routed via Unified CM. The administrator can define a list of domains to route SIP URI calls via Unified CM by selecting “*Only calls that match the specified (comma separated) domains”* and

then specifying the domains in the text box. All other calls will be made using native Webex calling service.

Note: All calls made by the user to a phone number will be routed via Unified CM.

ii. Validate DNS

The next step is to validate DNS configuration. It is assumed that DNS SRV records are already created for existing the Jabber deployment. Here you are simply verifying this configuration.

While on the corporate network, validate that the Unified CM record can be discovered for all Voice Services Domains. For example, *_cisco-uds._tcp.example.com*. DNS should return Unified CM node A records as configured with port 8443.

While outside the corporate network, validate that the Expressway-E record can be discovered for all Voice Services Domains. For example: *_collab-edge._tls.example.com*. DNS should return the Expressway-E node A records as configured with port 8443.

iii. Validate Unified CM and Expressway Settings

In general, the Webex App will use the same Unified CM and Expressway configurations in place with the existing Jabber deployment. The configuration aspects that are of specific interest for Webex include:

- Users and Authentication
- OAuth Settings
- Service Profiles
- Jabber-config
- Devices
- Device Security Profile
- Quality of Service
- Push Notifications

Users and Authentication

User accounts should already exist on Unified CM for the existing Jabber deployment. The Webex App will discover the user in Unified CM as shown in the following example:

> When alice@example.com signs into the Webex App, the application attempts to discover "alice" and "alice@example.com" during Unified CM home-cluster discovery.

SSO is highly recommended but not mandatory for Webex with Unified CM calling. SSO should be configured for Unified CM and Expressway, using the same IdP as used for SSO enablement of Webex. If SSO is enabled, Webex App users on Windows and Mac will only need to authenticate once at startup and will gain access to both Webex and Unified CM services. Users on Android and iOS will have to authenticate separately for Unified CM services even if SSO is enabled. This will be resolved in a future release of Unified CM.

If SSO is not enabled, users will need must manually authenticate to Unified CM after logging into the Webex App.

OAuth

It is a best practice to enable OAuth refresh token login flow on Unified CM and Expressway. The Webex App will store and utilize the OAuth refresh token in the same manner as Jabber.

- The OAuth refresh token can be presented to Unified CM/Expressway to authorize a user (gain access to Access token) without the need to re-authenticate every session
- The OAuth refresh token has a lifetime defined by Unified CM (default is 60 days)
- Webex App will delete the OAuth refresh token on sign out.

If OAuth Refresh Token Flow is not enabled on Unified CM, the Webex App will need to authenticate with Unified CM each time the user signs in.

Note: If SSO and OAuth Refresh Token Flow are not enabled on Unified CM, the Webex App can encrypt and store userID and password locally, so users do not need to manually reauthenticate each login.

If OAuth Refresh Token Flow is not enabled, secure SIP and media (for Unified CM calls) is not possible with the Webex App.

For more details on configuring OAuth Refresh flow in Unified CM and Expressway refer to the *Deploying OAuth with Cisco Collaboration Solution Release 12.0* whitepaper available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/jabber/11_9/Unified-CM-OAuth-Whitepaper-v17-FINAL.pdf.

Service Profiles

The Webex App relies on Unified CM Service Profiles to enable the following services:

- CTI (Desk phone Control Mode)

  The CTI profile defines the Unified CM server(s) within the user's cluster the Webex App should connect to for CTI services when the running in desk phone control mode.

- Voicemail (Unity Connection)

  The Voicemail profile defines the Unity Connection server(s) that the Webex App should connect to for visual voicemail services. If SSO is enabled for Unified CM, it must also be enabled for Unity Connection.

  If Unified CM and Unity Connection are not enabled for SSO, within the Voicemail Profile set the **Credentials source for voicemail service** *setting to Unified CM – IM and Presence.*

  The Webex App uses the Unified CM credentials to gain access to voicemail services.

The following profiles can be deleted as the Webex App will not read them:

- Conferencing profile
- MailStore Profile
- Directory Profile
- IM and Presence Profile

Jabber-config

The jabber-config information will also be read by the Webex App. The jabber-config can be accessed from the Service Profile in Unified CM 12.5 and above, or from the jabber-config.xml file on Unified CM 11.5 and earlier.

The Webex App will only read a subset of available Jabber parameters from the jabber-config file. The jabber-config file parameters read by the Webex App are specific to advanced calling functions such as Pickup Groups and Multiline. Webex App configurations for other services are managed from Control Hub. The existing jabber-config files/profiles can be minimized to the parameters relevant to the Webex App.

For a list of jabber-config parameters read by the Webex App refer to the *Deployment Guide for Calling in Webex (Unified CM)* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide.html.

The Webex App can read the jabber-config from any of the following:

- Jabber Client Configuration (jabber-config.xml) Profile
- Jabber-config.xml file
- Jabber-config-*<name>*.xml file as defined in the Cisco Support Field on the Device configuration page

Devices

The Webex App will utilize the same Unified CM device types for softphone mode as Jabber. It is recommended to enable each user for all device types. If a user is enabled for Unified CM calling in the Webex App, they will be presented with an error if the device type specific to their current platform is not available. It is important to consider Unified CM device capacity when adding devices to the system.

Device Security Profile

The Webex App does not support CAPF enrollment process to enable secure Unified CM calling. Organizations who are using CAPF enrollment to enable secure calling for Jabber, will need to migrate to SIP OAuth to enable secure Unified CM calling for the Webex App. SIP OAuth is available with Unified CM 12.5 and above. OAuth Refresh Token Flow must be enabled on Unified CM before enabling SIP OAuth.

Quality of Service (QoS)

The Webex App will mark packets with DSCP values for Unified CM calling, in the same way that Jabber does. DSCP settings will be read from the Unified CM Cluster Service Parameters by the Webex App running on Mac, iOS and Android.

For Windows devices DSCP values cannot be set by the Webex App and should be set via a Microsoft Group Policy.

Push Notifications

Enabling Push Notifications Services for Apple and Android devices is highly recommended when deploying the Webex App. If Push Notifications are already enabled for Jabber, there are no required changes when transitioning to the Webex App.

For more details on all of the above settings, refer to the *Deployment Guide for Calling in Webex (Unified CM)* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide.html.

iv. Contact Center Considerations

Users who require access to advanced contact center calling features may need to continue to utilize Jabber for calling services, until the Webex App supports advanced contact center features. Webex already supports Unified CM calling features that may be used in a contact center environment including Multiline, Hunt Groups, Pickup Groups, and Built in Bridge. However, certain features are only available in Jabber including:

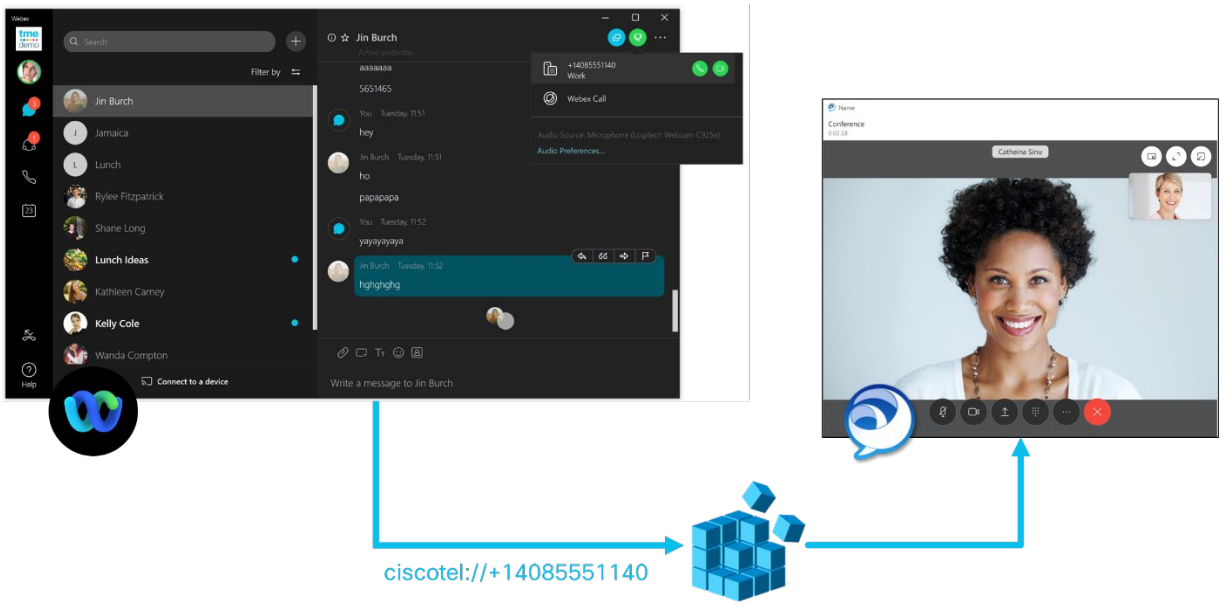
- Ad Hoc Call Recording
- Silent Monitoring
- Agent Greeting
- Whisper Announcement
- Supervisor Barge
- Recording Tone
- Zip Tone

If users require the features in the above list, those users can be enabled for the Webex App with cross launch to Jabber for calling. This is a mode where Jabber is cross launched when the user makes a call to a phone number or SIP URI from the Webex App. Users enabled for this mode will have access to all the above Jabber contact center calling features, while still using the Webex App as their primary collaboration tool. It is suggested to only enable this mode for the specific user groups who need access to contact center features.

The Webex App cross launches Jabber via the *ciscotel://* protocol handler. Jabber registers to the *ciscotel* protocol handler on Windows, Mac, iOS and Android. When a user makes a call to a phone number or SIP URI, the Webex App invokes *ciscotel://* with the phone number/SIP URI appended. This ensures the call is made using Jabber. The Webex App does not connect to Unified CM in this deployment mode.

Figure 32 details a user making a call using the Webex App. The Webex App invokes *ciscotel://* with this phone number. Jabber will then call this number and the conversation window will come to the foreground.

Figure 30. *Webex Cross Launch to Jabber for Calling via ciscotel://*



Incoming Unified CM calls will be received by Jabber.

To enable this mode for a user group, the following steps should be taken:

1. Set Webex App Calling Behavior to “Cisco Jabber app” for the user group.
2. Migrate user group to Jabber Phone-Only Mode.
3. Update jabber-config for user group.

Calling Behavior is defined in Control Hub. Calling Behavior should be set to “Cisco Jabber app” for user group who require advanced contact center calling features. This can be set on a per user basis in Control Hub or can be set in bulk using CSV file provisioning method discussed earlier in this document. If using

the CSV file provisioning method to enable Jabber cross launch, the column *Calling Behavior* should be set to *CALL_WITH_APP_REGISTERED_FOR_CISCOTEL* for the user group.

Users who will continue to use Jabber for calling can be migrated to Phone Only mode. Webex App will be used for messaging and meetings. To migrate users to Phone-Only mode from Full UC mode make the following changes in Unified CM:

- Users need to be disabled from IM & Presence Server – Uncheck *Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)*.
- IM & Presence should be removed from the Service Profile – Set IM & Presence Profile to **None** in the users Service Profile.

The user will receive a notification in Jabber that their configuration has changed and will need to sign in again to refresh configuration.

The jabber-config should be updated with the following settings for users who are enabled for Jabber Cross Launch from the Webex App.

Table 6 summarizes the jabber-config settings updates for users who are enabled for Jabber Cross Launch from the Webex App.

Table 6. *Jabber-Config Parameter Settings for Jabber Cross Launch*

Parameter	Configuration
<PresenceDomain>***example.com***</PresenceDomain>	Required for Phone Mode.
<EnableProximity>**false**</EnableProximity>	Webex App is the wireless pairing application.
<CalendarIntegrationType>**0**</CalendarIntegrationType> <MacCalendarIntegrationType>**0**</MacCalendarIntegrationType> <EnableCalendarIntegration>**false**</EnableCalendarIntegration>	Webex App will manage calendar integrations.

<Meetings_Enabled>**false**</Meetings_Enabled>	Webex App will provide meetings functionality.
<DockedWindowVisible>**false**</DockedWindowVisible>	Disable Jabber Docked Window.
<Start_Client_On_Start_OS>**true**</Start_Client_On_Start_OS>	Start Jabber when device starts up.
<EnableSIPURIDialling>**true**</EnableSIPURIDialling>	Turn on SIP URI dialing in Jabber.

For more details on the jabber-config file and the parameter settings, refer to the *Parameters Reference Guide for Cisco Jabber* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/cjab_book_parameters-reference-guide-for-cisco-jabber-14_0.html

For more information about cross launching Jabber from Webex, refer to the *Webex with Jabber Cross Launch* application note available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/mcp/APPLICATION_CALLING-Webex_with_Jabber_Cross_Launch.pdf.

4. Meetings: Understand meeting experience requirements

Meeting Webex Meetings App to Webex App transition will not be covered in detail in this document.

To enable Webex Meetings App experience within the Webex App the following requirement must be met:

- If Webex Meetings site is based on Site Admin, site linking must be enabled. For more information on site linking, refer to the *Link Cisco Webex Sites to Control Hub* article available at https://help.webex.com/en-us/341eud/Link-Cisco-Webex-Sites-to-Control-Hub.
- The Webex Organization must be enabled for the Webex Meetings experience within the Webex App. Contact your Cisco representative to have this enabled.

For more details on the meeting workload transition refer to the *Upgrade Webex Meetings App to Webex App* article available at https://help.webex.com/en-us/nda7hb0/Upgrade-Webex-Meetings-app-to-Webex-app.

Transition Steps and Considerations

Below is a summary of steps required for transitioning from Jabber to the Webex App.

Before proceeding you should back up your collaboration and infrastructure systems including Unified CM, if you must back out or abandon the transition.

This deployment guide assumes that administrators will push the initial Webex App package to desktop devices (Windows and Mac) using a deployment tool. Software upgrades will be managed either from Control Hub push or via administrative tool push.

Follow these transition steps to move from Jabber to Webex:

1. Review network and firewall requirements.

   The Webex App will connect to a range of services. The application will always make its primary connection to Webex. The Webex App may also connect to third-party services depending on what is enabled for the user (for example, Microsoft Office 365 if content management is enabled). The Webex App initiates outbound connections only. Webex service never initiates connections to the Webex App. Webex services are hosted in globally distributed data centers, that are either Cisco-owned or hosted in a Cisco Virtual Private Cloud on the Amazon AWS platform.

   The Webex App will also connect to Unified CM and corresponding services including Expressway (MRA) and Unity Connection (voicemail). It is assumed desktops and mobile devices will already have access to these services within the existing Jabber deployment.

   Ensure that all network requirements are met by referring to the *Network Requirements for Webex, Webex Meetings, and Cisco Jabber* article available at https://help.webex.com/en-us/WBX000029031/Network-Requirements-for-Webex-Webex-Meetings-and-Cisco-Jabber.

2. Integrate protocol handlers.

If the organization is using protocol handlers to integrate Jabber into third-party applications, changes may be required in those applications to move the integration to the Webex App. For example, a corporate directory web application may be configured to cross launch Jabber to make a call when a user clicks on a phone number. The application may be using *ciscotel://* protocol handler, which will launch Jabber and call the appended number. The application would need to be updated to use the *webextel://* protocol handler to cross launch the Webex App. Protocol handlers should be updated as shown in Table 7.

Table 7. *Protocol Handlers*

Function	Jabber Protocol Handler	Webex App Protocol Handler
Call	tel://	webextel://
Call	ciscotel://	webextel://
Call	sip://	sip://
Message	xmpp://	webexteams://im?email=

For more details on protocol handlers, refer to the *Webex | Add Links for Meetings or Spaces with webexteams Protocol* article available at https://help.webex.com/en-us/n5yzg8y/Webex-Add-Links-for-Meetings-or-Spaces-with-webexteams-Protocol.

3. Configure software updates.

Webex App updates are released on a monthly basis. The Webex App for desktop will query the Webex service for new updates and will automatically upgrade whenever an update is discovered. Organizations can set a custom update schedule if desired. The update schedule is set in Control Hub. Update frequency can be set to every 1 or 3 months. Once an update is available, the Webex App will download the update in the background. The user will receive a restart notification when

ready. A deferral period can be set which allows users some time before the application will automatically be updated.

Administrators can also download updated builds of the Webex App and push to desktops with third-party deployment tools if desired.

For more details on Webex update management, refer to the *Product Update Controls for Webex* article available at https://help.webex.com/en-us/wlgw73/Product-Update-Controls-for-Webex.

4. Deploy Webex App.

The Webex App can be pushed and installed on desktop devices via third-party deployment tools or can be installed manually by end users.

- The Webex App for Windows is installed via a .msi file.
- The Webex App for Mac is installed via a .dmg file.

When installing the Webex App on Windows devices, there are two different methods:

- Install the application for the current user.
- Install the application for all device users.

Installing the application for the current user is the default method. This does not require administrative privileges on the Windows device. When the Webex App is installed for current user, it is installed to the directory: *%LocalAppData%\Programs\Cisco Spark*.

To install the application for all device users, use the command line switch *ALLUSER=1* at install time. This method requires administrative privileges on the Windows device. When the Webex App is installed for all users, it is installed to the directory: *C:\Program Files\Cisco Spark*.

For more details on Webex App installation, refer to the *Webex | Installation and Automatic Upgrade* articles available at https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

The Webex App is installed and upgraded on mobile devices from public application stores, Google Play and Apple AppStore. The Webex App for desktop devices provides a QR code capability to direct users to the mobile application download page in the public application stores.

Note: If organizations wish to manage Webex App rollout on mobile devices via a Mobile Application Management (MAM) tool, they can get IPA and APK packages from Cisco.

For more details on using MAM for deploying Webex App, refer to the *Sign Up for the Mobile Application Management Program* available at https://help.webex.com/en-us/j6gys3/Sign-Up-for-the-Mobile-Application-Management-Program.

5. Contact and preferences migration.

Administrators can enable users who are migrating to the Webex App from Jabber with the Contacts and Preferences tool. This tool migrates the following data from Jabber to the Webex App:

- Contacts
  - Directory Contacts
  - Custom Contacts
  - Federated Contacts
- Preferences
  - Notification settings
  - Audio and Video device selection
  - Video preferences for incoming calls

This migration tool is built into Jabber and the Webex App for Windows or Mac. Users must be running a minimum version of Jabber, or they must have a patch installed to enable this tool. For information on the latest supported versions refer to the *Deployment Guide for Calling in Webex (Unified CM)* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide.html.

When the tool is enabled, Jabber will synchronize contacts list and preferences data to the Webex App on the local device. The Webex App will then write the data to the user profile service in Webex.

As shown in Figure 33, this tool can be enabled using the Jabber jabber-config file by using the *EnableJabber2TeamsMigration* parameter. The

WebexTeamsDownloadURL parameter can also be set which will take users to the Webex App download page if it is not already installed on the device.

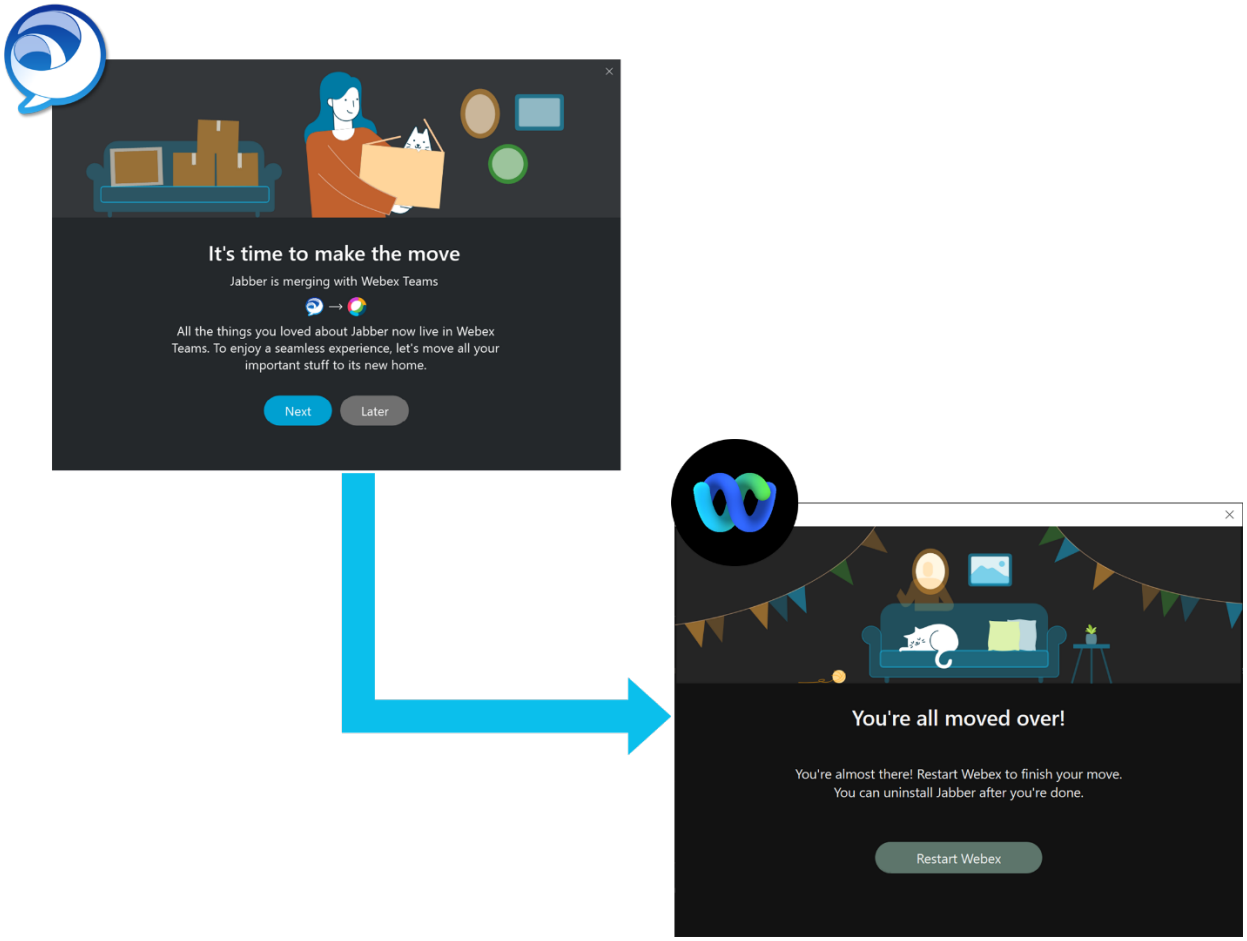
Figure 31. *Jabber-config to Enable Jabber to Webex Contacts & Preferences Migration Tool*

```
57
58  <Options>
59    <EnableJabber2TeamsMigration>true</EnableJabber2TeamsMigration>
60    <WebexTeamsDownloadURL>https://www.webex.com/downloads.html</WebexTeamsDownloadURL>
61  </Options>
```

When Jabber downloads the updated configuration file, the migration wizard will be presented to the user between 5 minutes and 3 hours later. The migration wizard can be manually started from the Jabber help menu.

Figure 34 shows portions of the Jabber to Webex migration wizard for contacts and preferences migration

Figure 32. *Jabber to Webex App Contacts and Preferences Migration*



6. Enable Outlook integration.

Both Jabber and the Webex App provide integrations to Outlook contact cards to view a user's presence and click to message/call. This integration is available for Windows and Mac.

This integration uses the *proxyAddress* attribute in AD. The *proxyAddress* attribute should be mapped to the Webex userID (email address). The address should be prefixed with *sip://*. For example:

> Alice's Webex ID is *alex@example.com*. The *proxyAddress* for Alice should be set to *SIP:alice@example.com*.

The *proxyAddress* should already be set if Jabber was previously integrated with Outlook. Ensure that the user address is correct for Webex deployment.

On Windows this integration is enabled via a registry setting. Only one application can integrate with Outlook at a time. Webex will not overwrite the existing Jabber Outlook integration at install time.

The administrator can enable the Outlook integration for Webex when the user is ready to have it disabled from Jabber by using the *regsvr32* utility available in Windows. Making this change will involve updating the registry. This will require administrative permissions on the device. This activity can be performed centrally by an administrator using a third-party tool such as Microsoft GPO.

For more details on the Outlook integration for Webex App, refer to the *Enable Webex Users' Status to Display in Microsoft Outlook* article available at https://help.webex.com/en-us/gk4yog/Enable-Webex-Users-Status-to-Display-in-Microsoft-Outlook.

Post Transition Steps and Considerations

After the transition is complete, there are additional optional steps you may wish to consider to clean-up the environment:

1. Remove Jabber client applications from user devices.

   Jabber can be uninstalled from devices manually or via third-party deployment tools.

   In the case of Jabber for Windows, Jabber can be installed using the command line switch: *msiexec.exe /x PATH_TO_CiscoJabberSetup.msi /quiet*

   Locally cached Jabber files can be removed from the user profiles. For example, in the case of Windows, the following directories would be deleted:

   - *%current_user%/AppData/Local/Cisco/Unified Communications/**
   - *%current_user%/AppData/Roaming/Cisco/Unified Communications/**

   Note: Any sensitive data stored in cache such as contact lists, call history is encrypted and can only be accessed with Jabber.

2. Archive Unified CM IM&P content.

   Before decommissioning Unified CM IM&P servers as well as third-party databases and file servers, consider archiving Unified CM IM&P content. The content that should be archived includes:

   - Jabber contact lists
   - Persistent chat
   - Managed file transfer

Jabber contact lists

Jabber contact lists are stored on Unified CM IM&P. Even though Jabber contact lists can be migrated to Webex using the migration utility discussed previously, it's good practice to export contact lists from the Unified CM IM&P cluster and store for some time after decommissioning the servers. This will ensure that users who might be on extended leave or that miss a migration window will be able to access their contact lists, even after Unified CM IM&P has been decommissioned. Contact lists can be exported using the BAT. For more information on exporting user contact lists with BAT refer to the "Bulk Administration of Contact Lists" chapter of the *Configuration and Administration of the IM and Presence Service, Release 12.5(1)* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/config

AdminGuide/12_5_1/cup0_b_config-and-admin-guide-1251/cup0_b_config-and-admin-guide-1251_chapter_011110.html.

Persistent chat

Persistent chat rooms and managed file transfer are optional services for Unified CM IM&P deployments. If either or both are enabled, an organization may want to archive the content before decommissioning.

Persistent chat room content is stored on a third-party database managed by the organization. This content can be retrieved from the database and archived using database tools. Consider archiving this content before decommissioning the databased or database server. For more information on the table structure of the database for backing up persistent chat room content refer to the "Database Tables" chapter of the *Database Setup Guide for the IM and Presence Service, Release 12.5(1)SU2* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/database_setup/12_5_1/cup0_b_database-setup-guide-1251su2/cup0_mp_edff2920_00_external-database-tables.html.

Managed file transfer

Managed file transfer content is stored on a customer-provided third-party file server managed by the organization. The content is stored on a fileserver in plain text by default. Encrypting fileserver stored content is recommended. Consider archiving managed file transfer content before deleting file transfer content or decommissioning the file server.

3. Decomission Unified CM IM&P server nodes.

When the Unified CM IM&P content is archived and assuming SIP federation is not required, the Unified CM IM & Presence server nodes can be decommissioned.

Users should be un-associated from Unified CM IM&P within Unified CM. Then, Unified CM IM&P nodes should be removed from the Unified CM cluster.

For more information on decommissioning Unified CM IM&P server nodes, refer to the "Manage the Server" chapter of the *Configuration and Administration of the IM and Presence Service, Release 12.5(1)SU2* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_5_1_su2/cup0_b_config-and-admin-guide-1251su2/cup0_b_config-and-admin-guide-1251su2_chapter_011100.html.

References

Calling in Webex Unified CM

- Webex Installation and Automatic Upgrade

  https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade

- Deployment Guide for Calling in Webex Unified CM

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

Collaboration Transitions

- Collaboration Transitions Program Page

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

- Transition Map for Transitioning from Jabber to Webex

  https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/mcp/TDM_CLIENTS_Jabber_to_Webex.pdf

Compliance and Policy

- Control Hub (Compliance) Datasheet

  https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740772.html

- Data Residency in Webex

  https://help.webex.com/en-us/oybc4fb/Data-Residency-in-Webex

- Set the Retention Policy for Your Organization

  https://help.webex.com/en-us/nqmr56k/Set-the-Retention-Policy-for-Your-Organization

- Block External Users in Webex Spaces for Your Organization

  https://help.webex.com/en-us/agrt8/Block-External-Users-in-Webex-Spaces-for-Your-Organization

Directory and Identity

- Ways to Add Users to your Control Hub Organization

  https://help.webex.com/en-us/nj34yk2/Ways-to-Add-Users-to-your-Control-Hub-Organization

- Add, Verify and Claim Domains

  https://help.webex.com/en-us/nxz79m5/Add-Verify-and-Claim-Domains

- Single Sign-On Integration in Control Hub

  https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Control-Hub

- Deployment Guide for Cisco Directory Connector

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

Hybrid Services

- Deployment Guide for Cisco Webex Hybrid Calendar Service

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/calendarservice/cmgt_b_deploy-spark-hybrid-calendar-service.html

- Deployment Guide for Cisco Webex Hybrid Data Security

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/datasecurity/cmgt_b_hybrid-data-security.html

- Deployment Guide for Cisco Webex Hybrid Messaging Service

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/messageservice/cmgt_b_spark-hybrid-message-deployment-guide.html

Meetings

- Upgrade Webex Meetings App to Webex App

  https://help.webex.com/en-us/nda7hb0/Upgrade-Webex-Meetings-app-to-Webex-app

- Add Links for Meetings or Spaces with webexteams Protocol

  https://help.webex.com/en-us/n5yzg8y/Webex-Add-Links-for-Meetings-or-Spaces-with-webexteams-Protocol

Messaging

- Federation for Webex

  https://help.webex.com/en-us/05i99o/XMPP-Federation-for-Webex

- SIP or XMPP Interdomain Federation for Webex

  https://help.webex.com/en-us/n8gtpu7/SIP-or-XMPP-Interdomain-Federation-for-Webex

Network

- Network Requirements for Webex, Webex Meetings, and Cisco Jabber

  https://help.webex.com/en-us/WBX000029031/Network-Requirements-for-Webex-Webex-Meetings-and-Cisco-Jabber

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**