MESSAGING

Transitioning from Unified CM IM&P to Jabber Team Messaging

Deployment Guide

August 27, 2019

Contents

Introduction

Target Audience

This migration document is intended to be used by teams who are currently running Cisco Jabber with Cisco Unified CM IM&P and are looking to migrate to Jabber team messaging mode. Jabber team messaging mode is a deployment model of Jabber, where calling is serviced by Unified CM, while messaging and presence services are serviced by the Webex Teams platform. There are links to other documentation throughout this document to assist.

Overview

Cisco Jabber is a modular UC client that can be deployed in a number of ways. Jabber provides for numerous collaboration workflows including:

- Softphone audio and video calling
- Deskphone control audio and video calling
- Messaging and Presence
- Contacts Integration
- Meetings
- Voicemail

Organizations can deploy Jabber to meet their requirements by enabling some or all of the above workflows. For example, Phone-Only mode is a deployment model of Jabber where messaging is disabled.

Messaging, presence, and meetings workflows can be serviced from the cloud or on-premises. For example, Jabber can utilize Webex Meetings (cloud) or Cisco Meetings Server (on-premises) for meetings service. Messaging and presence can be serviced from Unified CM IM&P (on-premises) or from Webex Messenger (cloud). Beginning with Jabber 12.6, the Webex Teams platform can also be utilized for messaging and presence.

Figure 1 shows an on-premises deployment model with Jabber enabled for calling, messaging, and presence services from Unified CM and Unified CM IM&P respectively.

Figure 1. On-Premises Jabber Deployment: Calling and Messaging/Presence

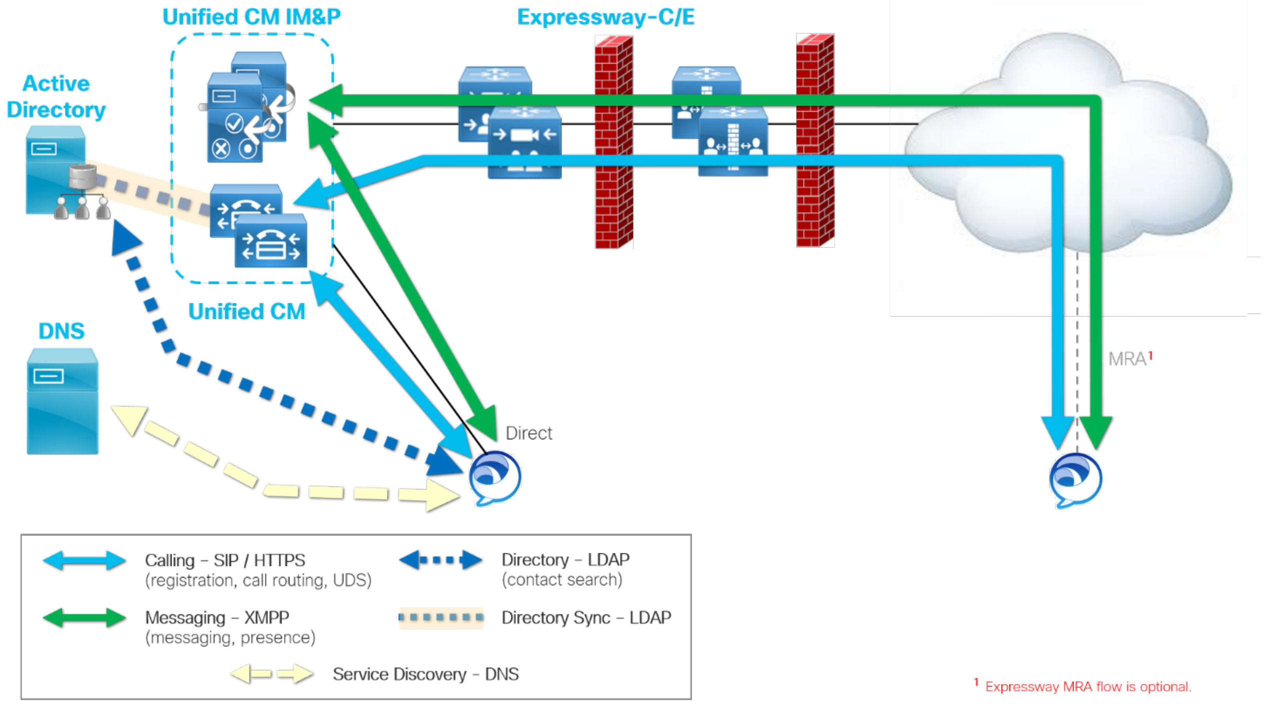


Table 1 lists the components used and functions provided with this on-premises calling, messaging, and presence deployment.

Table 1. On-Premises Deployment Components and Functions

Product	Description
Unified CM	Provides calling functionality to Jabber (softphone mode) via SIP. Unified CM also provides configuration and directory services via the UDS service (HTTPS).
Unified CM IM&P	Provides Jabber messaging and presence functionality via XMPP. Unified CM IM&P also provides contact list functionality to Jabber.
Expressway-C / E	Expressway Mobile and Remote Access enables Jabber clients to connect securely from outside the organization. Expressway is deployed in pairs to proxy external Jabber clients through the firewall.
Active Directory (any LDAPv3 directory)	Provides contact resolution and contact search capabilities to Jabber. Optionally, the LDAP directory may also be used to authenticate Jabber users.
Domain Name System (SRV Records)	Jabber uses Domain Name System (DNS) services to determine whether the client is inside or outside the coporate network by automatically discovering on-premises

	servers or Expressway Mobile and Remote Access points on the public Internet.

Jabber is a modular client. This means user services such as messaging can be added, removed, or migrated to a different service. This document focuses on the Jabber messaging service transition from Unified CM IM&P to Webex Teams. This deployment model is called Jabber team messaging mode.

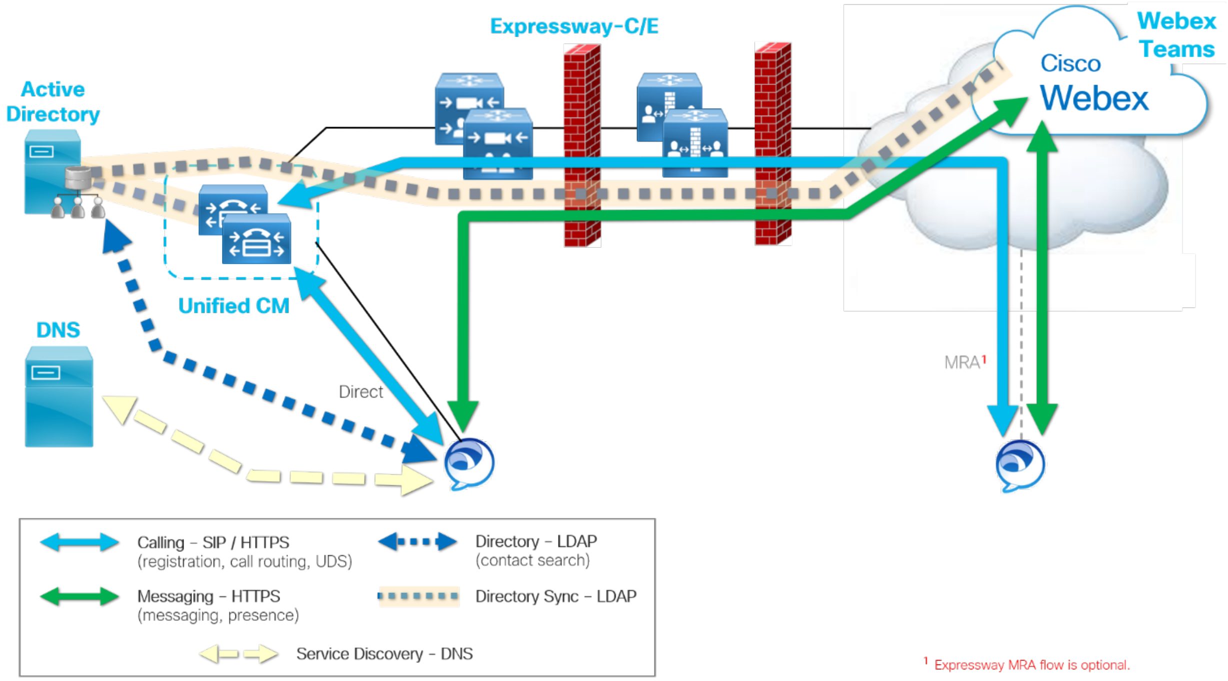
Deploying Jabber in team messaging mode provides numerous benefits including

- Persistent 1:1 and group space messaging along with file sharing without the need for dedicated external databases as required with Unified CM IM&P.
- Highly accessible Webex Teams API and bot framework interactions.
- Comprehensive views of the organization's utilization patterns and in-depth reporting and diagnostics with Webex Control Hub Analytics capabilities.
- Reduced total cost of ownership as messaging is serviced from the cloud. Unified CM IM&P, Persistent Chat database servers, and Managed File Transfer file servers are no longer required on-premises.

Note: Messages and groups persistently archived with Unified CM IM&P's persistent chat feature will NOT be migrated during the transition to Jabber team messaging. Persistent chat data may be archived to a read-only PDF that can be signed, secured, and shared as a reference ensuring important information is not lost.

Figure 2 shows the target deployment architecture with messaging and presence services delivered from the cloud (Webex) and calling delivered from on-premises (Unified CM).

Figure 2. Jabber Teams Messaging Deployment: On-Premises Calling and Cloud Messaging/Presence


Expressway-C/E
Webex Teams
Cisco Webex
Active Directory
Unified CM
DNS
Direct
MRA[1]
Calling – SIP / HTTPS (registration, call routing, UDS)
Directory – LDAP (contact search)
Messaging – HTTPS (messaging, presence)
Directory Sync – LDAP
Service Discovery – DNS
[1] Expressway MRA flow is optional.

Note: With this deployment Unified CM IM&P is no longer required.

Table 2 lists the components used and functions provided with this Jabber team messaging deployment.

Table 2. Jabber Team Messaging Deployment Components and Functions

Product	Description
Unified CM	Provides calling functionality to Jabber (softphone mode) via SIP. Unified CM also provides configuration and directory services via the UDS service (HTTPS).
Webex Teams	Provides messaging and presence functionality via HTTPS. Webex Teams also provides contact list functionality to Jabber.
Expressway-C / E	Expressway Mobile and Remote Access enables Jabber clients to connect securely from outside the organization. Expressway is deployed in pairs to proxy external Jabber clients through the firewall.
Active Directory (any LDAPv3 directory)	Provides contact resolution and contact search capabilities to Jabber. Optionally, the LDAP directory may also be used to authenticate Jabber users.

Domain Name System (SRV Records)	Jabber uses Domain Name System (DNS) services to determine whether the client is inside or outside the coporate network by automatically discovering on-premises servers or Expressway Mobile and Remote Access points on the public Internet.

Existing Architecture

Consider the following before beginning a transition to Jabber team messaging mode

- Service Discovery
- Authentication
- Directory Integration
- Contact List
- User Impact of Migration

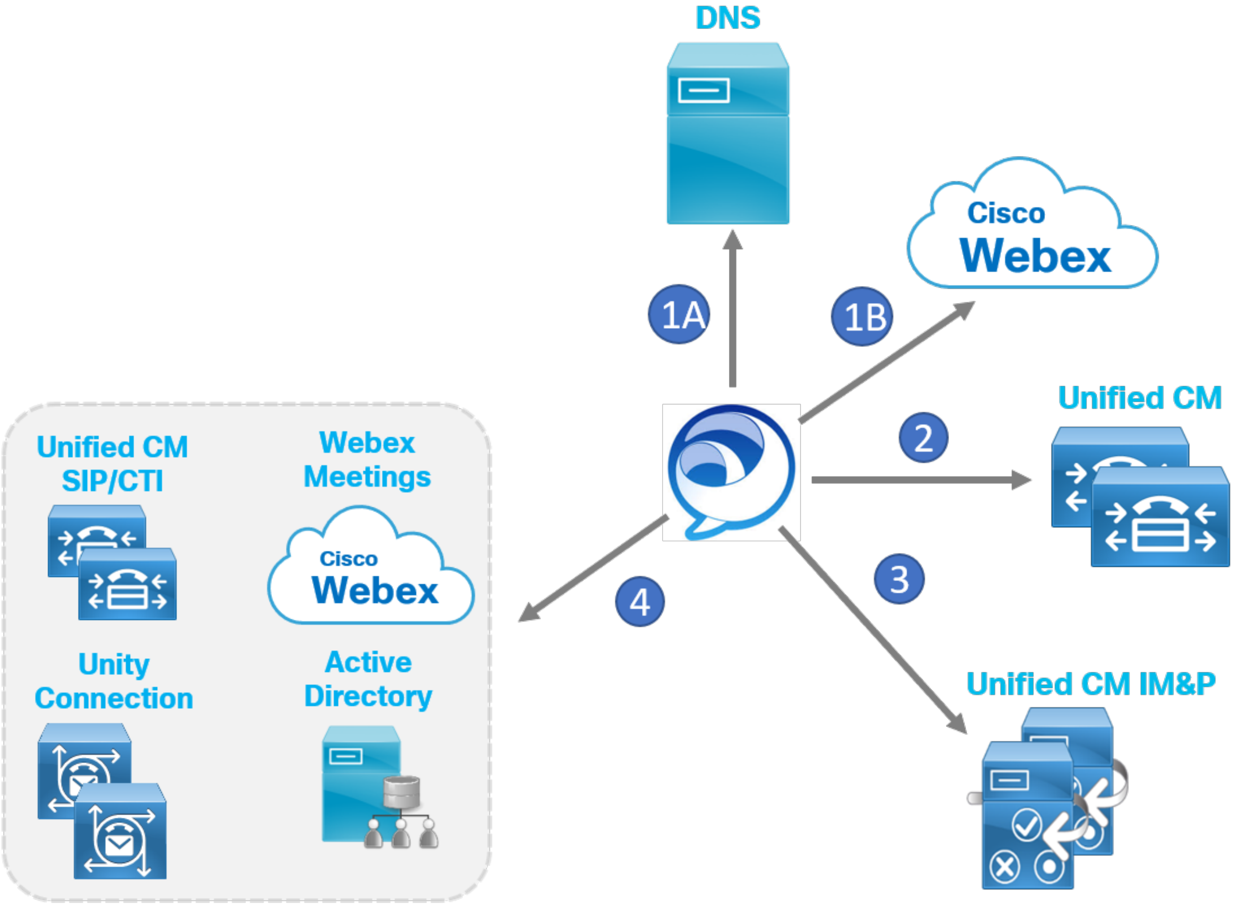
Each of these items should be understood for the existing on-premises Unified CM IM&P deployment first.

Unified CM IM&P Service Discovery

Figure 3 below details a first time Jabber login for an on-premises Unified CM / Unified CM IM&P deployment. First, the Jabber client sends a DNS SRV query to the DNS server for _cisco-uds._tcp.domain.com and _collab-edge._tls.domain.com (where domain.com is replace with the domain name for the deployment as specified by the user at sign in) (see Figure 3, step 1A). The DNS server should return a DNS A record for either Unified CM or Expressway-E, depending on whether Jabber is querying an internal or external DNS server. In this example, the DNS server is returning an A record for a Unified CM node based on the _cisco-uds._tcp.domain.com query.

Note: If the DNS server did not return a result for _cisco-uds, but did return a result for _collab-edge, Jabber would determine that it is outside the corporate network and attempt to connect to Expressway-E.

Figure 3. On-Premises Jabber Deployment: Service Discovery



Along with the DNS SRV queries, the Jabber client simultaneously sends a query to a Connect Authentication Service (CAS) Webex URL (for example, http://loginp.webexconnect.com/cas/ FederatedSSO?org=[domain_name]) (see Figure 3, step 1B). The query checks whether the domain and user are enabled for a Webex messaging service: Jabber team messaging mode OR Webex Messenger. Since this example deployment is UCM IM&P based, the domain/user will not be enabled for Jabber team messaging mode or Webex Messenger.

Next, Jabber queries the Unified CM node returned in the DNS A record to determine the Unified CM home cluster of the Jabber user (based on the username provided at initial sign-in) (see Figure 3, step 2). Determining the home cluster relates to multi-cluster deployments and requires Intercluster Lookup Service (ILS) to be enabled on all Unified CM clusters in the deployment. In a single cluster deployment, there is only one cluster which is the home cluster for all users.

Once Jabber determines the home cluster, it then connects to the home cluster Unified CM and retrieves the user's Jabber device configuration. The downloaded configuration includes information about User Profile, Service Profile, Jabber Config and Device

Profile for the Jabber device. The Service Profile details which services the user is enabled for and where Jabber should connect for these services. The Service Profile often includes information for multiple services including IM & Presence, Meetings, Voicemail, Directory, and CTI. The Jabber Config provides additional configuration and customization settings to the client (for example, custom tab or telephony feature enablement like call pickup tab). The Jabber Config settings are applied at login time.

As shown, in Figure 3, step 3, Jabber now connects to the Unified CM IM&P server that is configured in the Service Profile. Once connected to Unified CM IM&P, Jabber downloads the user's contact list and then connects to the presence and messaging services via XMPP.

Finally, the Jabber client connects to services that are configured in the Service Profile. Jabber connects to services that are configured in the Service Profile (see Figure 3, step 4). These services can include Webex Meetings, Unified CM CTI service, Unity Connection voice messaging service, and directory service.

Note: Jabber will not obtain its calling / SIP service location from the Service Profile. This information is obtained via device configuration.

Unified CM IM&P Authentication

Unified CM supports three types of authentication model

1. Basic Authentication

   With this model Unified CM acts as the authentication service. The user ID and password are sent to Unified CM from Jabber and compared against the user ID and password (Hash) that is stored in the Unified CM database.

2. LDAP Authentication

   With this model the Unified CM proxies the authentication to the configured LDAP server. This means Unified CM does not store user password information in its database.

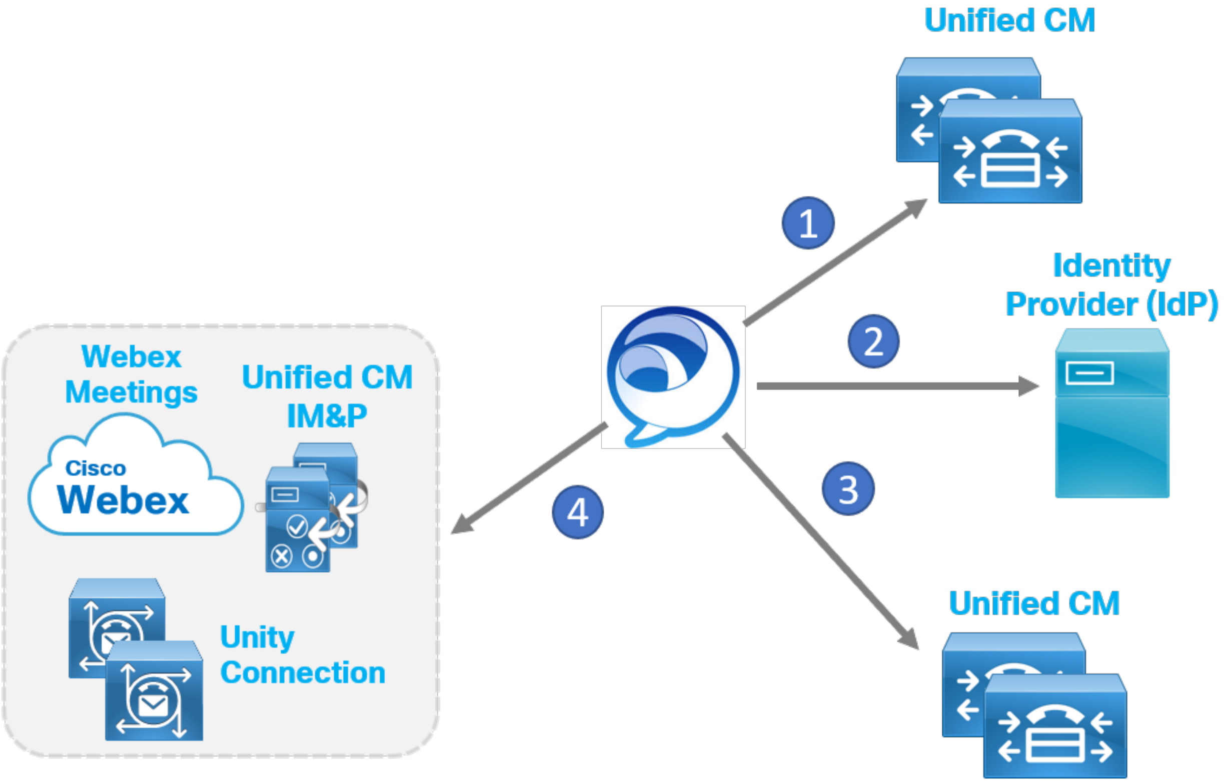
3. Single Sign On

   Single Sign On (SSO)involves a third-party server know as an Identity Provider (IdP). Unified CM supports the open standard SAML for SSO. This is also supported by Unified CM IM&P, Unity Connection and Webex. SSO enablement offloads authentication to the IdP. This means, by SSO enabling each service Jabber connects to, the services can be brought into the same authentication plane. The result for the user is that they need to only authenticate with the IdP once, and they will be able to access each collaboration service.

While Jabber team messaging mode can be implemented with Unified CM basic authentication or Unified CM LDAP authentication, because Jabber is modular and can connect to several different services simultaneously, generally it is recommended to enable SSO for all collaboration services within the deployment (Unified CM, Unified CM IM&P, Unity Connection, and Webex Meetings). For the rest of the document, it is assumed that SSO is enabled on Unified CM before transitioning to Jabber team messaging mode.

Figure 4 below details an on-premises Unified CM based login flow for Jabber. First, the Jabber client connects to specific Unified CM node based on the results of service discovery (Figure 4, step 1). Then, because Unified CM is SSO enabled, it is no longer responsible for user authentication. Instead, Jabber is redirected to the Identity Provider (IdP).

Figure 4. On-Premises Jabber Deployment: User Authentication



Next, as shown in Figure 4, step 2, the Jabber client authenticates with the IdP. The client offloads authentication to a system resource when SSO is enabled. The system resource is usually the native browser authentication engine (for example, Jabber for Windows offloads to Internet Explorer authentication engine). The system resource leverages the authentication engine to connect to the IdP which prompts the user for whatever authentication method is enabled on the IdP (for example, username and password). The user authenticates and if successful receives a Security Assertion Markup Language (SAML) assertion from the IdP. The SAML assertion can be provided to a service that is SSO enabled, with the same IdP, to gain access to that service.

Now, Jabber requests access to Unified CM services using the SAML assertion it received from the IdP previously. The Jabber client provides the SAML assertion to Unified CM (see Figure 4, step 3). Assuming the assertion is valid, Unified CM grants Jabber access. Once access is granted, the Jabber client downloads the configured Service Profile from Unified CM.

Finally, as shown in Figure 4, step 4, Jabber begins connecting to the service or services specified in the downloaded Service Profiles. For example, Jabber connects to services like IM & Presence (Unified CM IM&P), meetings (Webex Meetings) and voice messaging (Unity Connection). Assuming these services have also been SSO enabled, Jabber is able to use the SAML assertion previously obtained from the IdP to gain access to these other services. And, because of the SAML assertion, the user does not need to explicitly authenticate to each service individually.

Directory Integration

Jabber relies on a Directory Integration for numerous functions.

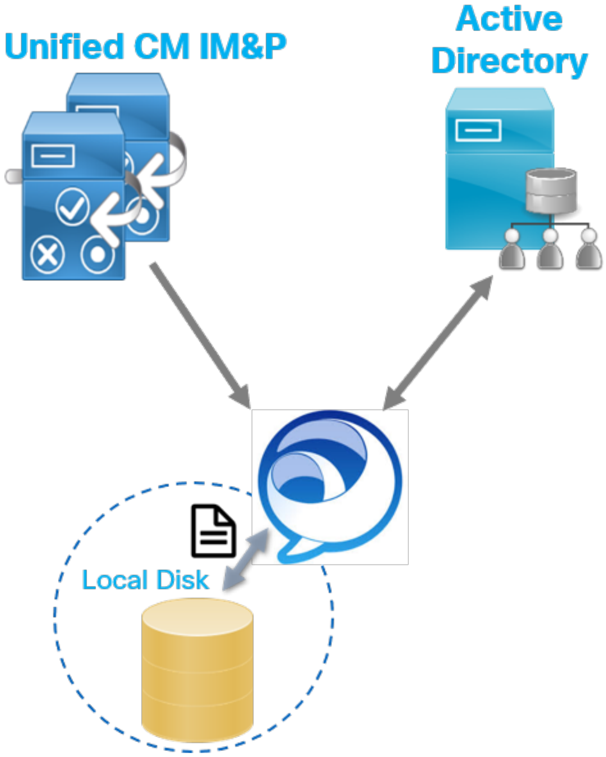
- Contact Resolution
- Directory Search
- Number Resolution

In a Unified CM IM&P based deployment, the Jabber client can utilize an LDAPv3 server or Unified CM User Data Services (UDS) as its directory service. On-premises Jabber clients can connect directly to LDAP or UDS. Jabber clients connecting via MRA will utilize UDS as their directory service. Unified CM UDS Proxy feature can be enabled to proxy UDS directory queries to LDAP. Jabber clients retrieve the directory profile from a Service Profile. The most commonly deployed directory server is Active Directory.

Contact List

In a Unified CM IM&P based deployment, the Jabber client retrieves its contact list from the Unified CM IM&P server. Jabber retrieves the contact list in the form of Jabber IDs (JIDs). Jabber then resolves the JIDs to DisplayName using Active Directory. The directory photo, phone numbers, and other identity information are also retrieved from Active Directory. Jabber writes the contact list to a local cache file on the device. At startup the Jabber client reads the cache file containing the contact list, this ensures faster login times as well as offline mode login. This cache file will be used to migrate contacts to Jabber team messaging mode.

Figure 5. On-Premises Jabber Deployment: Contact List



Client User Experience

Jabber 12.7 introduces a new user experience (UX) to align with the Webex Teams application. Prior to this UX alignment, the Jabber client typically operated in a two-window mode with the conversation window separate from the main client contacts window. The new UX puts contacts and conversation in a single window pane. Another UX alignment introduced with Jabber 12.7 was dark mode for the desktop client which is a software option that makes the overall user interface darker. It changes light backgrounds to a dark color and changes text from dark to light. The UX alignment of Jabber and Webex Teams will simplify an application transition in the future, if desired (Jabber to Webex Teams application).

Transition

Consider the following during the transition to Jabber team messaging mode

- Licensing Requirements for Team Messaging Mode
- Webex Control Hub
- Team Messaging Mode Authentication
- Team Messaging Mode Service Discovery
- Directory Integration in Team Messaging Mode
- Contact Lists in Team Messaging Mode
- Completing the Transition
- Post Transition

Licensing Requirements for Jabber Team Messaging Mode

Flex licensing is required for Jabber team messaging mode. Flex licensing allows users to consume Cisco cloud and on-premises services together. Ensure Flex Licensing is being used with your deployment before proceeding.

Webex Control Hub

In order to proceed, ensure you have acquired a Webex Teams organization. You must have a Webex Teams organization to access Webex Control Hub which is the administrative portal for Webex Teams services. Webex Control Hub is available at https://admin.webex.com/.

Enabling SSO for the Webex Teams organization is recommended, but the procedure for setting up SSO with Webex Teams is not covered in this document. Details are available at https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Cisco-Webex-Control-Hub

There are a few methods for provisioning user accounts. Directory Connector is the recommended approach. Deploying Directory Connector is not covered in this document. 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

You will enable Jabber team messaging mode using Webex Control Hub, however, before enabling, it is important to understand the Jabber team messaging login flow.

Jabber Team Messaging Mode Authentication

In team messaging mode, Jabber can connect to several different services

- Webex Teams
- Unified CM (on-premises calling)
- Webex Meetings
- Unity Connection (voice messaging)

Without SSO enablement, the user will need to perform manual authentication (enter their username and password) with each of these services individually. The login flow would be as follows:

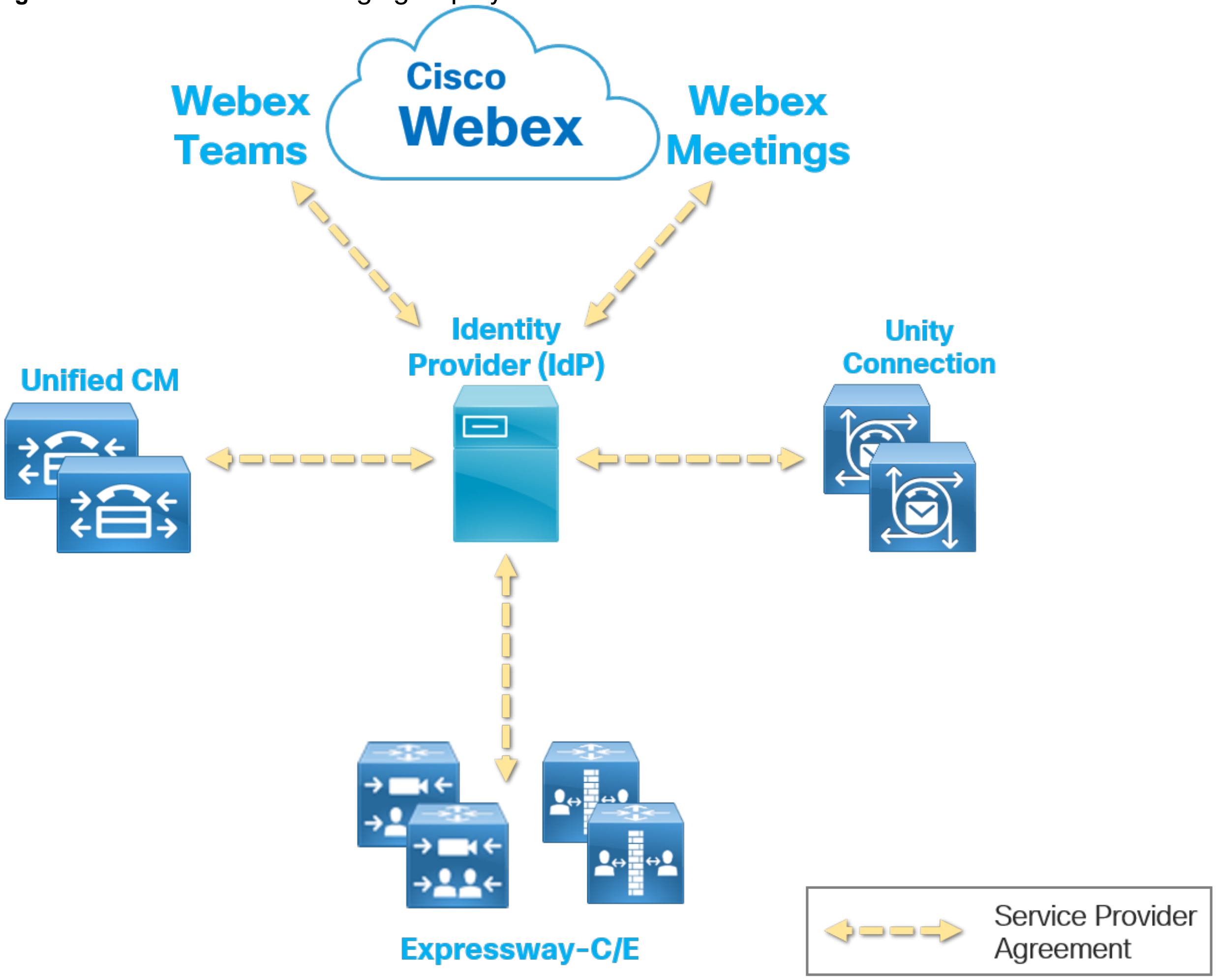
1. User manually authenticates with Webex Teams service
2. User manually authenticates with Unified CM
3. User manually authenticates with Webex Meetings
4. User manually authenticates with Unity Connection

Asking a user for multiple manual authentications is a poor user experience and will lead to issues and complaints. Further, without SSO, Jabber team messaging mode is not capable of OAuth Refresh Token Support or SIP OAuth.

Before migrating to Jabber team messaging mode it is highly recommended you enable SSO for the following components:

- Webex Teams Organization
- Webex Meetings
- Unified CM
- Unity Connection
- Expressway-C/E (MRA)

Figure 6. Jabber Team Messaging Deployment: User Authentication



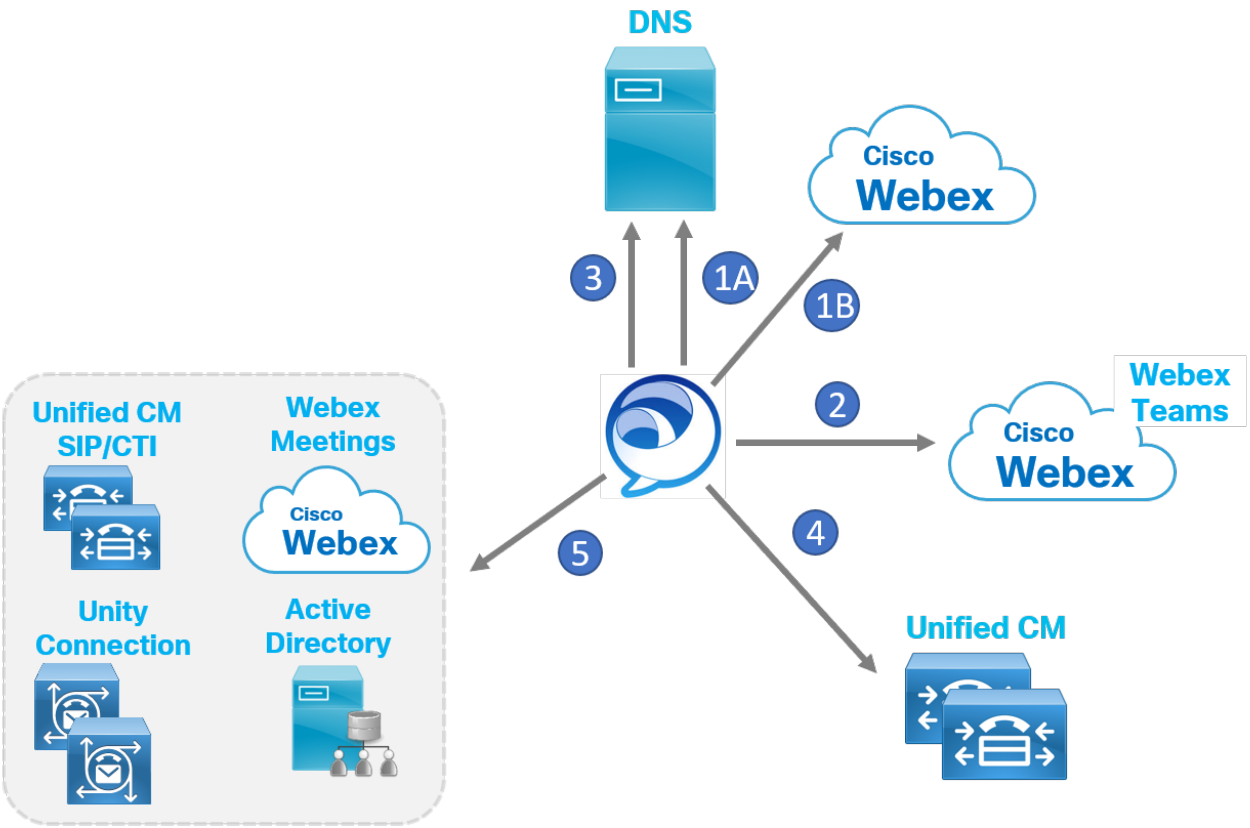
With SSO enabled on all services, the user will need to perform an initial manual authentication. Once authenticated, Jabber will use the SAML Assertion received from the IdP to authenticate with each service automatically.

Jabber Team Messaging Mode Service Discovery

In Jabber team messaging mode, the Webex Teams service is the primary authenticator. This means, at first time login, Jabber will connect to the Webex Teams service first, and then connect to Unified CM, followed by the voice messaging and meetings services.

As shown in Figure 7, the discovery flow begins with the simultaneous DNS SRV and Webex CAS queries sent from the Jabber client (step 1A and 1B). As previously discussed, Jabber queries for _cisco-uds and _collab-edge DNS SRV records based on domain entered by the user at startup. Likewise, the Webex discovery query is sent for the same domain with the user ID entered by the user at startup.

Figure 7. Jabber Team Messaging Deployment: Service Discovery



Assuming the domain (and user) are enabled for team messaging mode, the Jabber client will connect to the Webex Teams service (Figure 7, step 2). The user authenticates via SSO and the client then connects to Webex Teams services for messaging, presence and contact list. Jabber downloads a configuration setting for the Voice Services Domain. This is set by the admin and details the domain to perform DNS SRV discovery of Unified CM. (The configuration of Voice Services Domain is discussed later in this document).

The Jabber client performs a second DNS SRV query to the same DNS server using the Voice Services Domain received from Webex Team (Figure 7, step 3). Based on the results of this second DNS lookup, Jabber will connect to either Unified CM or Expressway-E (MRA).

If the DNS server returns a result for _cisco-uds, the Jabber client will connect to the Unified CM server returned in the result (Figure 7, step 4). Jabber will then perform full home cluster discovery on Unified CM based on the user ID. Just like an on-premises deployment, the client will be redirected to the user's home cluster where it will connect to a Unified CM node and download configurations (User Profile, Service Profile, Jabber Config, Device Config). Jabber will use the SAML Assertion already received from the IdP to authenticate with Unified CM with no user action required (assuming SSO is enabled).

In the case of MRA where DNS server returns a result for _collab-edge, the Jabber client will connect to Expressway-E which will forward inside to Expressway-C which proxies the Unified CM home cluster discovery and configuration file download on behalf of the Jabber client.

Once the Service Profile is applied, Jabber connects to services configured in the service profile (for example, Webex Meetings, Voicemail, and so on). Jabber will use the SAML Assertion already received from the IdP to authenticate with Webex Meetings and Unity Connection. Again, no user action is required (assuming SSO is enabled).

Note: Beginning with Jabber 12.7, it is possible to host a jabber-config.xml in Webex Control Hub. The Jabber client will download the jabber-config file from Webex Control Hub, if enabled. As a best practice, it is recommended to use the Jabber Configuration tool (Unified CM 12.5 and later) and Unified CM Service Profiles to configure and manage jabber-config.xml. In the case of Messaging Only mode, the jabber-config.xml must come from the Webex Control Hub.

Directory Integration in Jabber Team Messaging Mode

Just like a Unified CM IM&P based deployment, Jabber team messaging mode relies on a directory integration for things like contact resolution and directory lookups.

The Jabber client integrates with both Webex Teams and LDAP/UDS for directory service. Directory Integration in Jabber team messaging mode is flexible and can be configured in different ways, however, the integration defaults for various directory functions are as follows:

- Contact Resolution

  The Jabber client will resolve Display Name and directory photo/avatar from Webex Teams. The client will query LDAP/UDS to retrieve additional contact information such as phone number(s), job title, and so on.

- Directory Search

  When performing a predictive directory search in team messaging mode, Jabber searches against Webex Teams and LDAP/UDS. Common results (a user found via both searches) are merged to a single result.

- Number Resolution

  Number resolution from an incoming call is performed against LDAP/UDS.

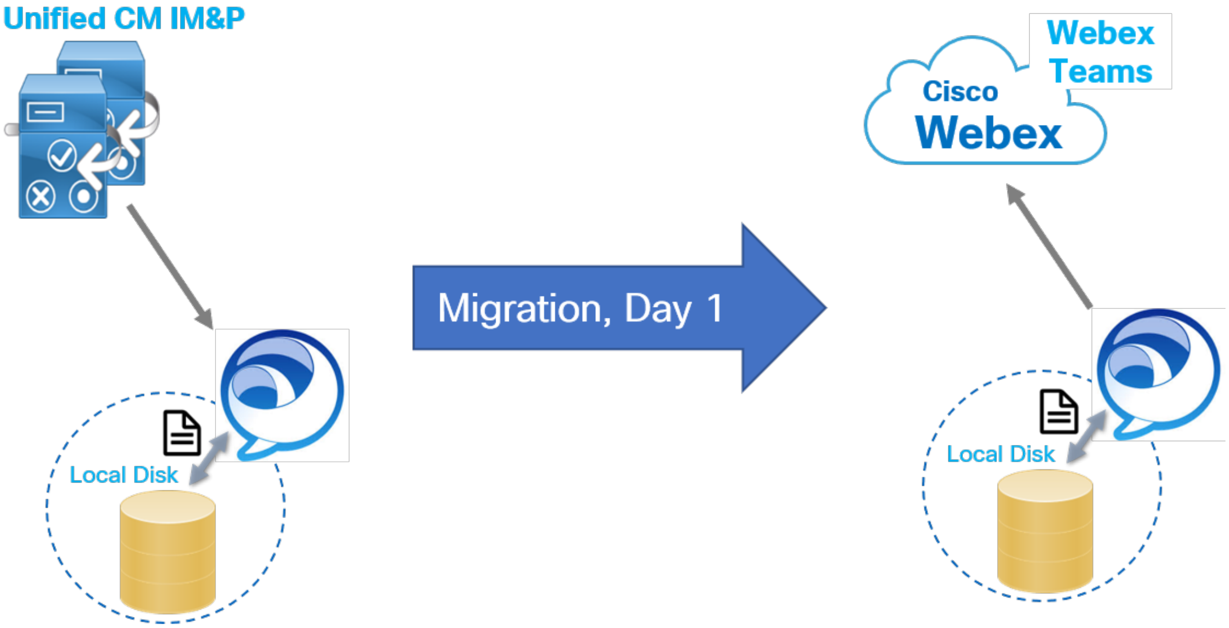
Additional configuration may be applied to specify non-default directory integrations. For example, Jabber could be set to perform predictive directory search against Webex Teams ONLY. This configuration might be used for an organization that chooses not to integrate with LDAP/UDS.

Jabber team messaging mode will retrieve its directory integration configuration from the Directory Service Profile in Unified CM.

Contact Lists in Jabber Team Messaging Mode

Webex Teams provides a contact list service for Jabber team messaging mode. As shown in Figure 8, contact list migration is supported from Jabber Unified CM IM&P mode to Jabber team messaging mode. Contact list migration is enabled by the administrator.

Figure 8. Jabber Team Messaging Deployment: Contacts Migration



Contact list migration from Unified IM&P mode to team messaging mode is implemented by Jabber. It is a client-side migration, meaning there is no direct migration of contacts from Unified IM&P to the Webex Teams service. Contact list migration works as follows:

- In Unified CM IM&P mode, the Jabber client downloads the users contact list from the Unified IM&P server and caches the list to disk.

- The administrator enables Contacts Migration for users migrating to team messaging mode.
- When Jabber migrates to team messaging mode, the client reads the contacts cache file, and writes the information to the Webex Teams contact service database. This is a one-time occurrence, that happens on day 1 of the transition.
- Jabber can now retrieve the Contacts List in team messaging mode (from Webex Teams service).

Note: Contact list migration is only supported with Jabber desktop clients (Windows and Mac). Contacts migration relies on Jabber having a contacts cache present on disk. This means Jabber should NOT be reset before migration.

Note: Contact list migration is only supported for deployments where the Webex Teams org domain matches the existing on-premises Services Domain (_cisco-uds /_collab-edge domain).

Completing the Transition

Once the previously mentioned pre-transition steps have been taken, including engaging Flex Licensing, acquiring a Webex Teams organization, enabling SSO (recommended) for Webex Teams organization and Unified CM, and synchronizing users to Webex Team platform (Directory Connector recommended), you are ready to initiate the transition to Jabber team messaging mode.

This transition involves the following steps:

1. Enable Jabber Team Messaging Mode for Webex Teams Organization

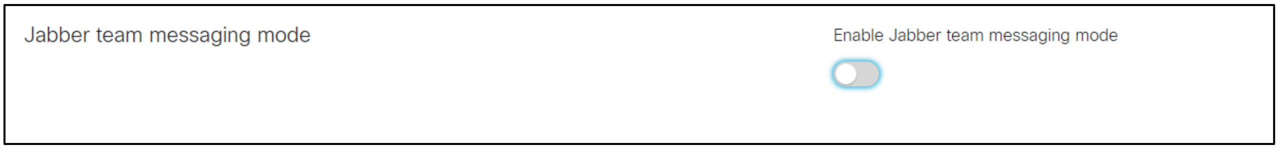
2. Enable Jabber Team Messaging Mode for Users

3. Service Discovery and First Connection to Jabber Team Messaging Service

Enable Jabber Team Messaging Mode for the Webex Teams Organization

The transition is initiated by the administrator enabling Jabber team messaging mode in Webex Control Hub (https://admin.webex.com/). This begins with running the team messaging mode wizard by navigating to **Services > Messaging** and clicking the toggle *Enable Jabber team messaging mode* (see Figure 9).

Figure 9. Jabber Team Messaging Deployment: Webex Control Hub - Enabling Jabber Team Messaging

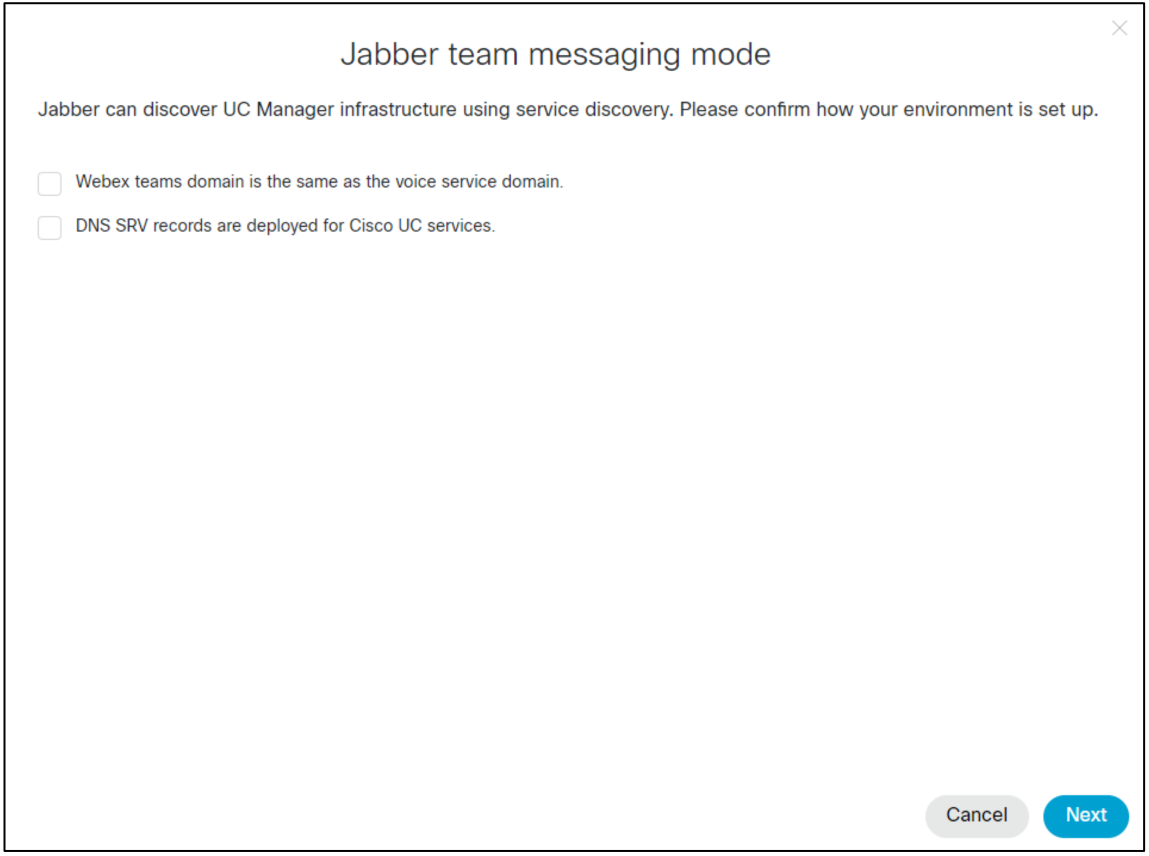


Jabber team messaging mode

Enable Jabber team messaging mode

As shown in Figure 10, this initiates the wizard which begins with UC Manager service discovery settings for team messaging mode.

Figure 10. Jabber Team Messaging Deployment: Webex Control Hub - Service Discovery Environment



Jabber team messaging mode

Jabber can discover UC Manager infrastructure using service discovery. Please confirm how your environment is set up.

□ Webex teams domain is the same as the voice service domain.

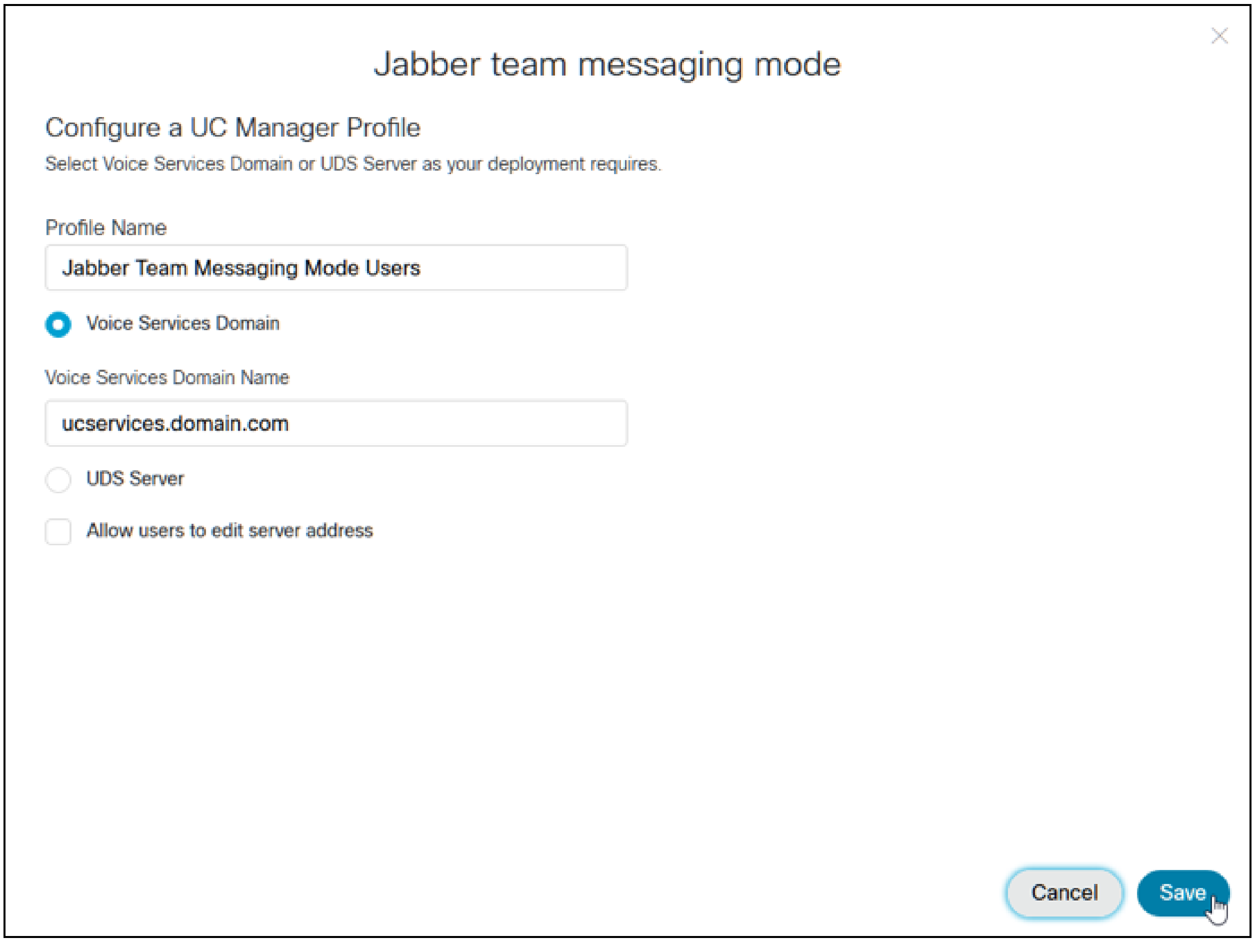
□ DNS SRV records are deployed for Cisco UC services.

If the **Webex Teams domain is the <u>same</u> as the domain where _cisco-uds and _collab-edge SRV records are deployed**, <u>check both boxes shown in Figure 10</u> and click **Next.** Jabber will perform Service Discovery for Webex Teams and Voice Services on the same domain.

If the **Webex Teams domain is <u>different</u> from the domain where _cisco-uds and _collab-edge SRV records are deployed**, leave the '*Webex teams domain is the same as the voice service domain*' unchecked, but check '*DNS SRV records are deployed for Cisco UC services*' (assuming you have already deployed DNS SRV records as recommended). Then, click **Next.**

In the final window of the wizard, specify a Profile Name, for example, **Jabber Team Messaging Mode Users** (see Figure 11). This profile can be assigned to individual users or groups of users. Next, specify the appropriate domain in the Voice Services Domain Name field. This is the domain where the _cisco-uds and _collab-edge SRV records are deployed. Click **Save**.

Figure 11. Jabber Team Messaging Deployment: Webex Control Hub – UC Manager Profile



Jabber team messaging mode

Configure a UC Manager Profile

Select Voice Services Domain or UDS Server as your deployment requires.

Profile Name: Jabber Team Messaging Mode Users

● Voice Services Domain

Voice Services Domain Name: ucservices.domain.com

○ UDS Server

□ Allow users to edit server address

The Jabber client will retrieve the Voice Services Domain configuration at login time and perform DNS SRV discovery against that domain. Full home cluster discovery will be performed against the Unified CM node returned by DNS.

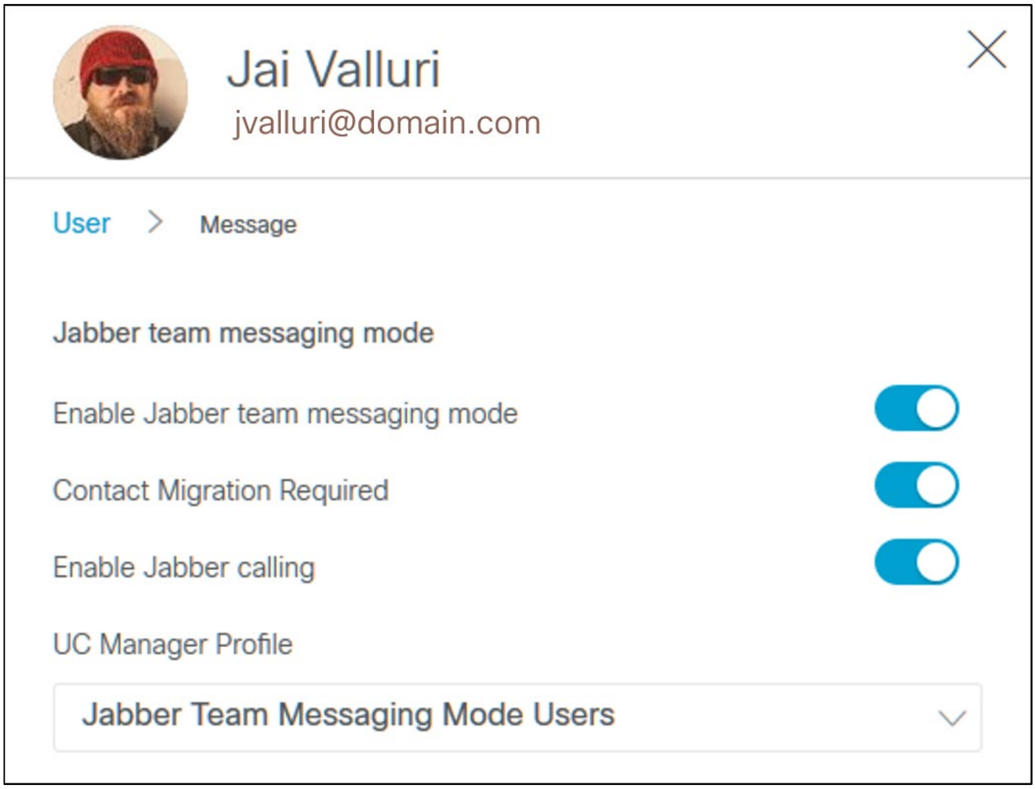
Note: There is an option to specify the actual Unified CM node that Jabber will connect to after connecting to Webex Teams. This can be enabled by clicking the *UDS Server* radio button in the wizard window and specifying the FQDN of the Unified CM node. With this setting, Jabber will bypass home cluster discovery. It is recommended to use the Voice Services Domain setting instead of specifying a static Unified CM UDS server.

Enable Jabber Team Messaging Mode for Users

With Jabber team messaging mode services now enabled for the Webex Teams organization, Jabber team messaging mode needs to be enabled at a user level. This can be performed by the administrator in bulk via a comma-separated values (CSV) file or can be done on a per user basis.

Figure 12 shows enabling Jabber team messaging mode for an individual end user (in this case, Jai Valluri). To enable on a per user basis, select a specific user from the Users tab. On the right-hand Services window, select Messaging.

Figure 12. Jabber Team Messaging Deployment: Webex Control Hub – User Services



Jai Valluri
jvalluri@domain.com

User > Message

Jabber team messaging mode

Enable Jabber team messaging mode: On

Contact Migration Required: On

Enable Jabber calling: On

UC Manager Profile: Jabber Team Messaging Mode Users

You will first enable the toggle for '*Enable Jabber team messaging mode*'. This will set the user's Jabber client to discover Webex Teams during Service Discovery. Next, if contact list migration (as previously described) is desired, enable the toggle for '*Contact Migration Required*' (see Figure 12).

Finally, enable the toggle for '*Enable Jabber calling*' (see Figure 12) if the Jabber client will also connect to on-premises Unified CM for phone services while in team messaging mode. Select the UC Manager Profile previously created during the wizard process (Jabber Team Messaging Mode Users). Jabber team messaging mode is now enabled for this user.

Service Discovery and First Connection to Jabber Team Messaging Service.

Once the administrator enables Jabber team messaging mode in Webex Control Hub for a user or group of users, the Webex Teams service will become discoverable by Jabber clients.

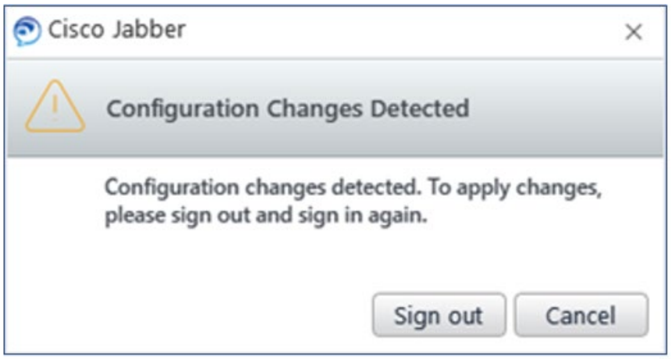
Jabber clients perform Service Discovery at the following intervals:

- Each time the Jabber client starts up from a zero-config state (no cached configuration).
- Between zero and 5 mins after Jabber start up from a cached configuration state.
- A random time every 7 to 9 hours whenever Jabber is running.

At the next Service Discovery interval, the Jabber client will send the usual discovery queries: Webex CAS and DNS SRV (_cisco-uds and _collab-edge)

Because Jabber team messaging mode is now enabled, the client detects this and notifies the user that the configuration has been updated and prompts them to sign out (and then sign in again) to refresh their configuration (see Figure 13).

Figure 13. Jabber Team Messaging Deployment: Jabber Configuration Change Detection



Cisco Jabber

Configuration Changes Detected

Configuration changes detected. To apply changes, please sign out and sign in again.

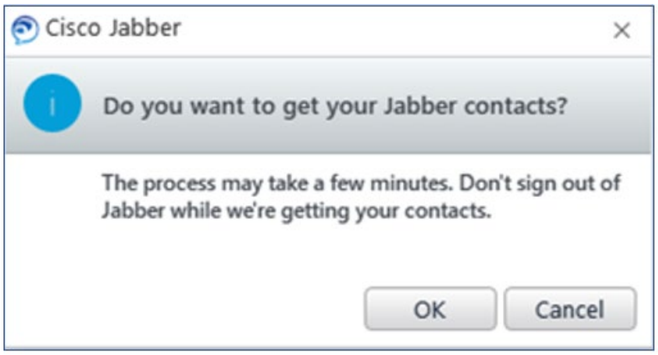
Once the user clicks **Sign out**, the client will sign out of services (Unified CM, Unified CM IM&P, and other services such as voicemail and meetings if enabled).

Next, the Jabber client connect to the Webex Teams service, and receive an authentication challenge (SSO is recommended). Once the user provides appropriate authentication credentials, Jabber is able to successfully connect to Webex Teams. The Jabber client then applies the two other configuration parameters set in Webex Control Hub previously when you enabled the user for Jabber team messaging mode:

- Contact Migration Required

If *Contact Migration Required* was set when you enabled the user for Jabber team messaging, the user is prompted to migrate their contacts as shown in Figure 14.

Figure 14. Jabber Team Messaging Deployment: Jabber Contacts Migration Prompt



Cisco Jabber

Do you want to get your Jabber contacts?

The process may take a few minutes. Don't sign out of Jabber while we're getting your contacts.

If the user clicks OK, Jabber will read the contact list cache on the local disk and write the contact list to the Webex Teams contact list service. The contact list is now imported into Webex Teams and will be available when a user logs into Jabber team messaging mode from desktop or mobile devices.

Note: Contact migration is only supported on with desktop Jabber clients (Windows or Mac). If the user clicks Cancel to the Jabber contacts migration dialog, they will be presented with the same option on next login and will continue to be presented with this option until they click OK.

- Enable Jabber calling

  If *Enable Jabber calling* is not set, client login is complete. Jabber will not attempt to connect to Unified CM.

  If *Enable Jabber calling* is set, Jabber will perform a second DNS SRV discovery based on the Voice Services Domain specified in the UC Manager Profile you created previously (Jabber Team Messaging Mode Users, see Figure 11).

  Jabber should discover either Unified CM or Expressway (MRA) depending where the client device and user are located. For example, if Jabber is on-premises and discovers _cisco-uds SRV record, it will attempt to connect directly to Unified CM.

  If Unified CM is SSO enabled, the Jabber client will use the existing SAML Assertion (obtained during the Webex Teams service authentication leg) to authenticate. The authentication happens in the background. The user does not need to manually authenticate. (If SSO is not enabled on either Webex Teams or UCM, the user will need to open the Jabber Options>Accounts menu to enter Unified CM credentials manually).

Once Jabber successfully signs in to Unified CM, the Service Profile is downloaded, and the client connects to Meeting, Voicemail, CTI, and other services. Jabber will also register to Unified CM in softphone mode, if enabled.

This user is now migrated to Jabber team messaging mode. Enable Jabber team messaging at larger scale by migrating users in bulk with a CSV file template. Details on this method of bulk user input is available at https://help.webex.com/en-us/e2okky/Modify-Users-in-Cisco-Webex-Control-Hub-with-the-CSV-Template

Post Transition

After the transition is completed, Jabber clients will receive phone services from Unified CM and messaging services from Webex Teams.

Once all users have been migrated to Jabber team messaging mode consider the following post-transition steps:

1. Remove unused Unified CM IM&P clusters.

   Now that users have been fully migrated away from Unified CM IM&P, all Unified CM IM&P cluster nodes should be decommissioned as they will no longer be used.

2. Remove unused database / file servers.

   Now that users have been transitioned off Unified CM IM&P, there is no longer any need for Persistent Chat database servers or Managed File Transfer file servers. These resources can be removed as they are no longer used, nor are they accessible, by Jabber clients within the deployment. Chat histories stored in Outlook folders are no longer written to by Jabber clients but will still be available.

References

Directory Connector Deployment

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

SSO Enabling Unified CM

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_0_1/cucm_b_saml-sso-deployment-guide-1201/cucm_b_saml-sso-deployment-guide-1201_chapter_010.html

SSO Enabling Webex Teams

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

User Modification via CSV

https://help.webex.com/en-us/e2okky/Modify-Users-in-Cisco-Webex-Control-Hub-with-the-CSV-Template

Webex Control Hub Information

https://help.webex.com/en-us/nuylwki/Cisco-Webex-Control-Hub

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.**