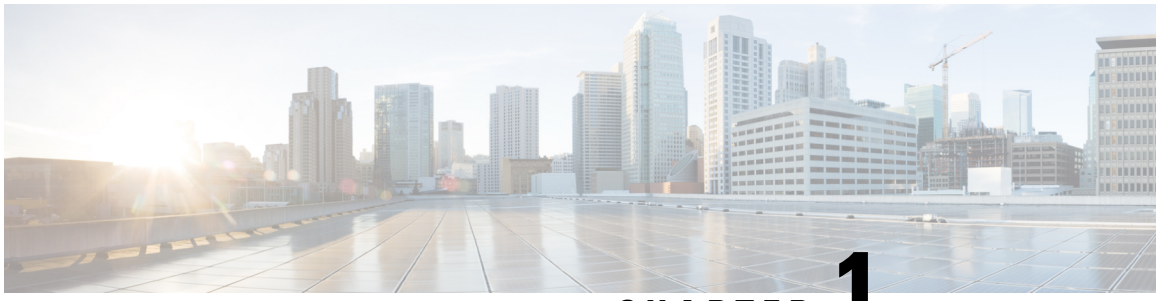
Deployment Guide for Hybrid Message

First Published: 2018-01-24

Last Modified: 2023-03-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

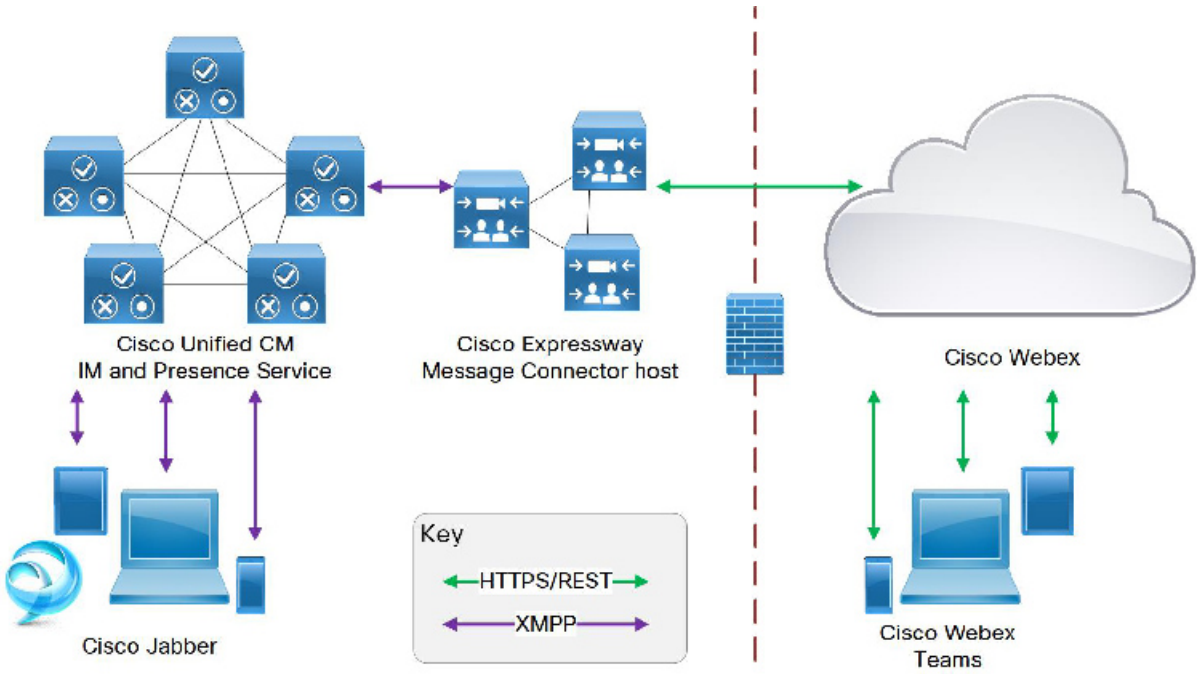
Cisco Webex Hybrid Message Service Overview

Hybrid Message Components and Users

Hybrid Message connects your Unified Communications Manager IM and Presence Service (IM and Presence Service) to Webex to enable interoperability with Webex App.

Note This deployment provides interoperability between your *on-premises Jabber deployment* and Webex App users. This is different to the interoperability between *cloud-based Jabber deployments* and Webex App users (see https://help.webex.com/article/nzx9su0 for more on that deployment).

Figure 1: Hybrid Message Components



On the left of the diagram is your on-premises deployment of Cisco Jabber and IM and Presence Service. On the right is your organization in Webex, with your Webex App users. You manage this organization using Control Hub.

The Hybrid Message enables interoperability between these two groups of users. The components that make Hybrid Message possible are the message connector, hosted on Cisco Expressway infrastructure on your premises, and the Message Service, running in the Webex cloud.

Licensing and Entitlement Factors Affecting Interoperability

- We assume that all users are previously licensed for Cisco Jabber, with Jabber registered to Cisco Unified Communications Manager IM and Presence.
- You need any paid-for Webex app offer for your organization. You can order this through Cisco Commerce Workspace.

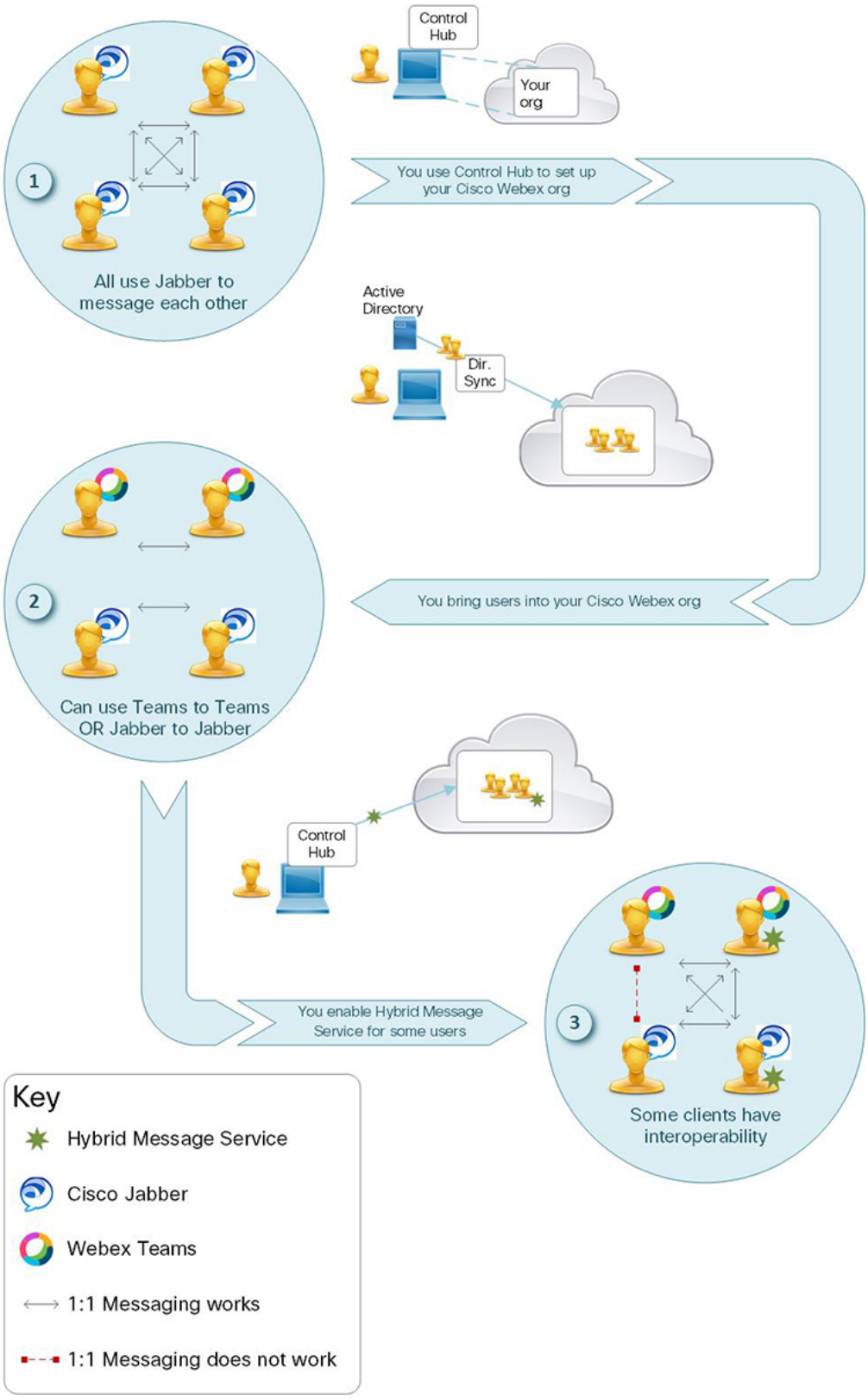
  You also need to have access to Cisco Webex Control Hub, with administrator privileges for your organization (you get these as part of the ordering process).
- You should import all Jabber users into Control Hub and grant them all the "Message Free" entitlement. This entitles all the Jabber users to the basic Webex App messaging functionality.

  There are no additional paid license requirements for this basic messaging. Having this entitlement for all users improves interoperability between those who are enabled for Hybrid Message and those who are only licensed for Jabber.
- Hybrid Message can only work between users who are in the same organization in Control Hub. The service does not enable Webex App users to communicate with Jabber users outside of their organization.
- Users who are enabled for Hybrid Message can use Jabber or Webex App to chat with all other users in the organization, irrespective of whether the recipient is using Webex App or Jabber.

- Users who are not enabled for the Hybrid Message can use Jabber to chat with all other users in the organization. They can use Webex App to chat with users who are enabled for Hybrid Message, but the messages are not copied to the recipients' Jabber clients.

User Interactions

Figure 2: Interoperability Between Clients During Implementation


Control Hub
Your org
You use Control Hub to set up your Cisco Webex org
1
All use Jabber to message each other
Active Directory
Dir. Sync
2
Can use Teams to Teams OR Jabber to Jabber
You bring users into your Cisco Webex org
Control Hub
You enable Hybrid Message Service for some users
3
Some clients have interoperability
Key
Hybrid Message Service
Cisco Jabber
Webex Teams
1:1 Messaging works
1:1 Messaging does not work

This diagram shows the progression of your user population as you implement Hybrid Message Service. At the start, all users are on Cisco Jabber (point 1 on diagram). The diagram then shows the tasks that you perform to get to the destination, where you have Hybrid Message Service enabled for some of your users (Point 3).

Now there are four ways to *send* chat messages:

- A user without Message Service uses Webex
- A user without Message Service uses Cisco Jabber
- A user with Message Service uses Webex
- A user with Message Service uses Cisco Jabber

The recipients can also use those four ways to *receive* chat messages, which means 16 possible interactions. You can expect eight of them to work because they are interactions between the same clients (Jabber to Jabber or Webex to Webex—point 2). Of the remaining eight interop scenarios, we expect three cases to fail:

Figure 3: Eight Scenarios for One-to-one Messaging

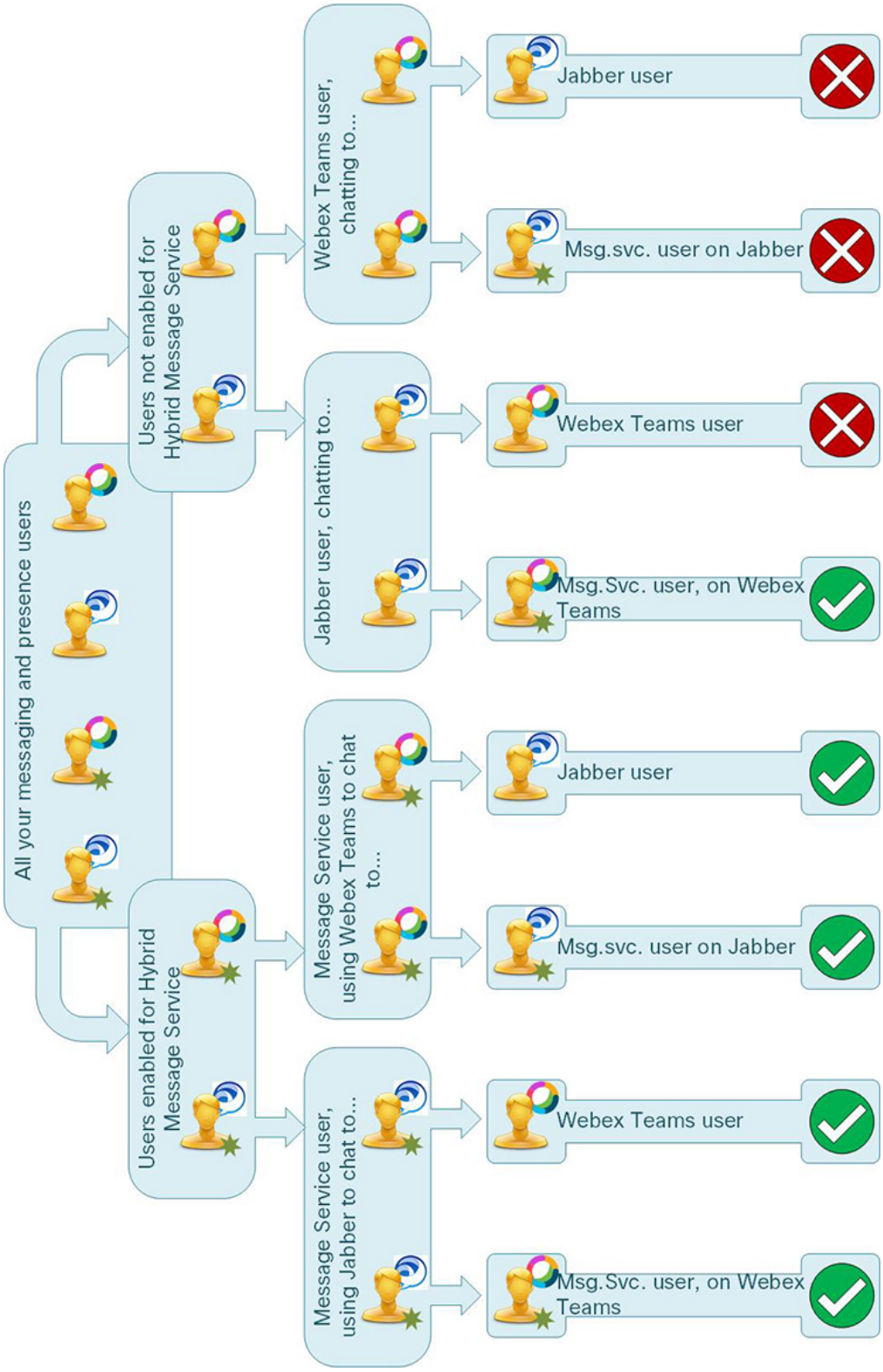
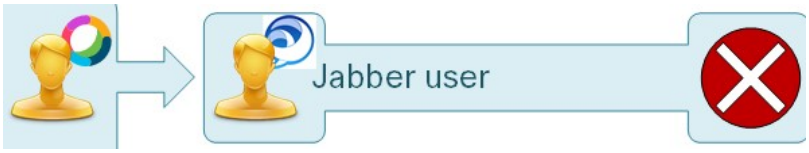


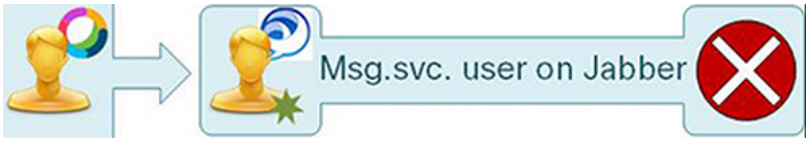
Figure 4: Expected failure: Webex to Jabber, neither user has Hybrid Message Service



The sender is using Webex but is not enabled for Hybrid Message Service. The sender uses Webex to start a direct space with the recipient. The recipient is using Jabber, so does not see the messages in Webex.

If the sender were enabled for Hybrid Message Service, the Webex chat messages would be copied to IM and Presence and sent from the Jabber account. But, because the sender is not enabled for Hybrid Message Service, the messages are not copied to IM and Presence, and so the recipient will not see them unless they use Webex.

Figure 5: Expected failure: Webex to Jabber client of a Hybrid Message Service user



The sender is using Webex but is not enabled for Hybrid Message Service. The sender uses Webex to start a direct space with the recipient. The recipient is enabled for Hybrid Message Service but is using Jabber, so does not see the messages.

This behavior is expected. We designed the service this way to reduce load, because we anticipate that you will enable Hybrid Message Service for the "early adopters" in your organization, and that they will use Webex as their primary chat client.

Figure 6: Expected failure: Jabber to Webex, neither user has Hybrid Message Service

The sender is using Jabber and starts a chat with the recipient's Jabber contact. The recipient is using Webex and does not see the Jabber conversation. The recipient is not enabled for Hybrid Message Service, so those Jabber messages are not copied and sent to Webex.

The recipient remains unaware of the conversation unless they use Jabber. In that case, if offline storage is disabled, the recipient may never see the conversation.

Deployment Models

Choosing a Deployment Model

Consider the following factors when choosing how you deploy Hybrid Message:

- Scale: How many IM and Presence Service users do you expect to serve? Will you need to add nodes / clusters to improve the capacity of the service to meet that requirement?

  We support 195,000 users per organization across multiple Expressway clusters.

We also support up to 5,000 Message Service users per Small Expressway, up to 6,500 users per Medium Expressway, and up to 15,000 users per Large Expressway. This gives a maximum number of 75,000 on a cluster of 6 Expressways, because the capacity of one node is reserved for redundancy. See https://help.webex.com/article/nv5p67g for an explanation of the Message Service capacity.

- Availability: How important is service availability to you? Do you need to deploy redundant nodes / clusters to ensure continuous service in the event of a failure?
- Geography: Global distribution of users means that you may have data centres in multiple timezones. Latency may be a factor to consider when choosing where to deploy your connector hosts.
- In each deployment scenario, remember that:
  - Each Expressway cluster has up to six nodes, including the primary.
  - You must register the primary node of each Expressway cluster with Webex.
  - To connect an Expressway cluster to an IM and Presence Service cluster, enter the publisher's details on the primary node of the relevant Expressway cluster. This action connects all nodes of the Expressway cluster with all nodes of the IM and Presence Service cluster (diagrams show only the primary to publisher connections, for clarity).

    You must not connect all Expressway clusters to all IM and Presence Service clusters. We do not support this scenario, because the potential benefit from redundancy is outweighed by the risk of overloading the solution.

    You must not associate multiple Expressway connector clusters with one IM and Presence Service cluster (even though your IM and Presence Service cluster may be able to home more message and presence users than your Expressway cluster can support). We do not support this scenario.

    You may connect multiple IM and Presence Service clusters to each Expressway connector cluster.

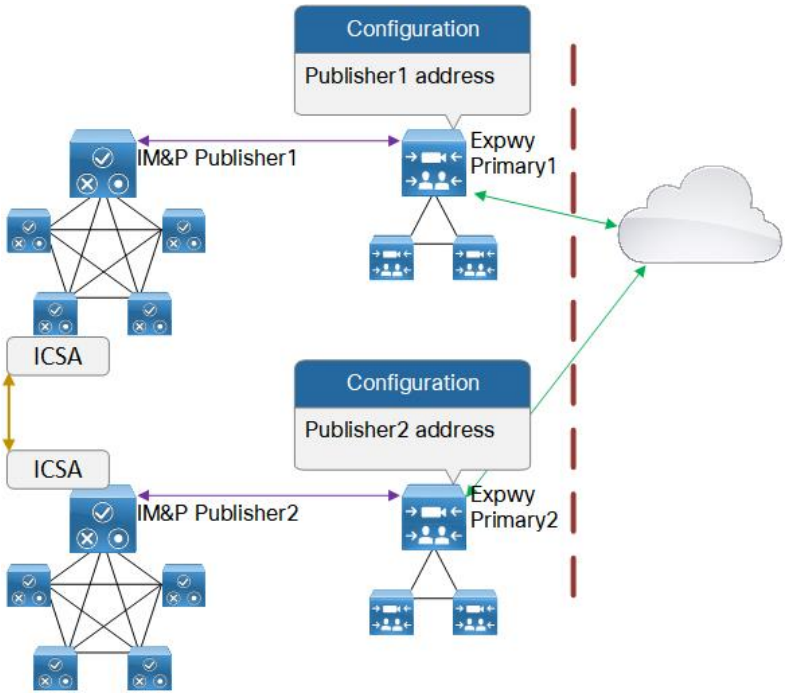
    We support up to 5 IM and Presence Service clusters per Expressway connector cluster.
  - You can use Resource Groups in Control Hub to define your organization's geography, and then assign Expressway resources to different resource groups that represent locations.

    The set of users you assign to each resource group should correspond to the users in all IM and Presence Service clusters served by the Expressways in those resource groups.

One Expressway Connector Cluster to One IM and Presence Service Cluster

This is the recommended deployment option. It requires an Expressway connector cluster per IM and Presence Service cluster. If you have more than one site, you can repeat the configuration in each datacentre (For example, two datacenters shown below).

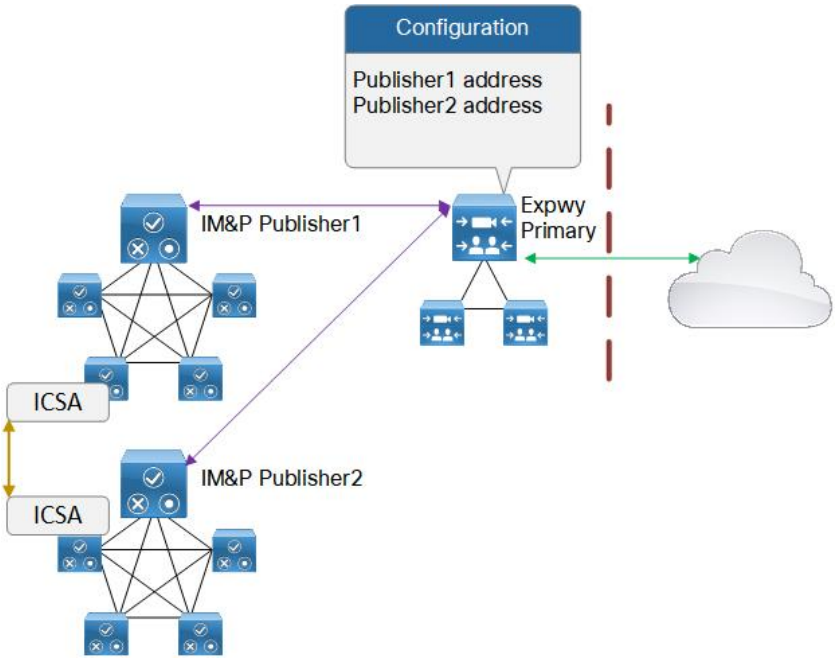
Figure 7: One to One Expressway to IM and Presence Service Cluster



One Expressway Connector Cluster to Multiple IM and Presence Service Clusters

This deployment option requires one Expressway connector cluster across the whole IM and Presence Service deployment. This option is simple to configure and manage, but scalability and latency could be concerns if you have many users and/or wide geographical distribution.

Figure 8: One Expressway Connector Cluster to Multiple IM and Presence Service Clusters



Meshing is Not Supported

There is a performance impact for each message connector that connects to an IM and Presence Service cluster. For that reason, we do not support multiple Expressway clusters connecting to one IM and Presence Service cluster. By extension, meshing the connectors with the IM and Presence Service clusters is not supported.

Figure 9: Not supported: Multiple Expressway Connector Clusters to One IM and Presence Service Cluster

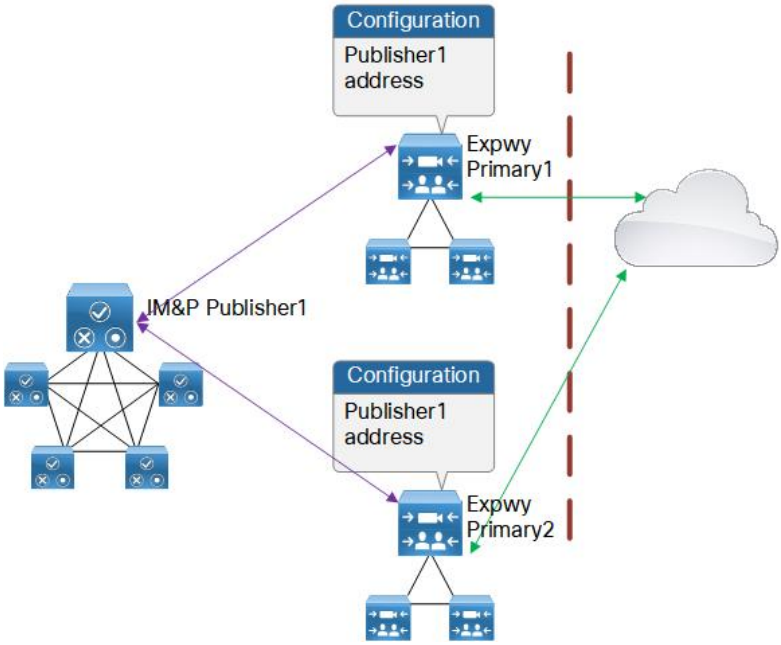
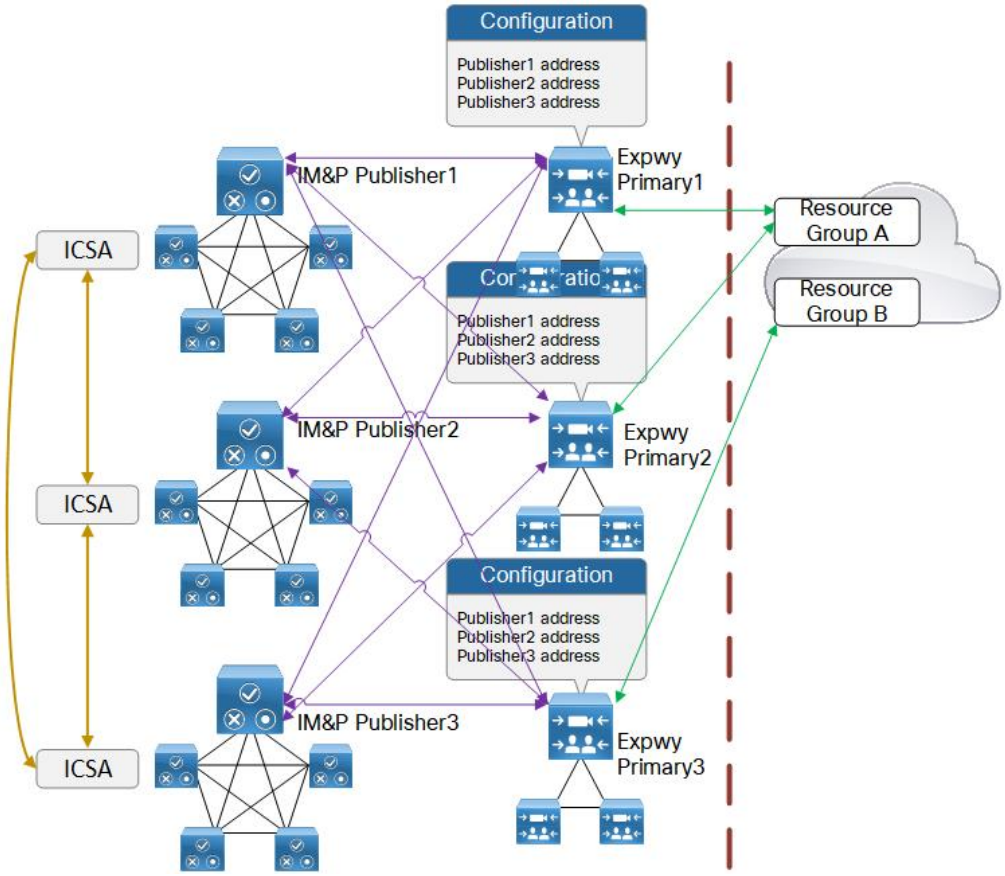


Figure 10: Not supported: Meshing Multiple Expressway Connector Clusters to Multiple IM and Presence Service Clusters



Scope of Deployment Features

Feature	Description
Webex for Government environment	Hybrid Message service is available in the Webex for Government environment.
Instant Messaging Compliance	Hybrid Message can work with IM and Presence Service that is configured for compliance. Webex App does not support compliance and Webex App to Webex App messaging is possible for blocked Jabber users.

Feature	Description
Message encryption	Supported (mandated) between your premises and Webex. • Messages from IM and Presence Service to Webex App are encrypted by the message connector. • Messages from Webex App to IM and Presence Service are decrypted by the message connector. • message connector makes TCP connections to IM and Presence Service nodes. TLS is not supported on these connections.
Multiple on-premises domains	message connector works with multiple XMPP domains.
Coresidency with other Hybrid Services	The Message Connector supports coresidency with other Expressway-based Hybrid Services (Hybrid Calling and Hybrid Calendar). Coresidency reduces the number of Hybrid Message users carried by the connector host. See https://help.webex.com/article/nv5p67g for details of coresidency and capacity.
Data Security / Key Management System	The Hybrid Message is compatible with Hybrid Data Security. We normally use the Webex Key Management System (KMS) for securing Hybrid Message, but you have the option to use an on-premises instance of KMS with Hybrid Message. See https://www.cisco.com/go/hybrid-data-security for details of Hybrid Data Security deployment.
Coresidency with Mobile and Remote Access (MRA)	We do not recommend installing Message Connector on an Expressway cluster that is used for MRA. However, if you do choose to do this, we will only support up to 100 Message Service users per node, to a maximum of 500 per cluster.
Deployment scale	We currently support up to 195,000 users per organization enabled for Hybrid Message, across multiple Expressway clusters. This limit applies to the subset of users in your organization that use Hybrid Message. It does not affect the number of users that you enable for Webex App; you should import all your Jabber users to Webex. See https://help.webex.com/article/nv5p67g for details of Hybrid Message scale and coresidency. You can deploy up to 5 IM and Presence Service clusters with one Expressway connector cluster. We do not recommend using multiple connector clusters with one IM and Presence Service cluster.

Feature	Description
XMPP or SIP messaging federation between the Jabber deployment and another domain	Hybrid Message service works when you have interdomain federation between the IM and Presence Service and a third-party messaging provider. This means that when a contact in a federated organization sends a message to a Hybrid Message user, the message appears to that user in both Jabber and the Webex App. **Note** XMPP or SIP federation with Hybrid Message service is not supported in the Webex for Government environment.
High availability and failover of IM and Presence Service nodes	The Message Connector is aware of the high availability setting on Presence Redundancy Groups. It responds automatically to failover / fallback events.
Webex for Government: Hybrid Message to enable interoperability between Webex App and Jabber	Hybrid Message is a service that enables interoperability between Jabber users and Webex App users. This service provides an option for migrating users from Jabber, connected to IM & Presence on your premises, to Webex App. Users who are enabled for this service can use the Webex App to read and respond to messages from Jabber users.

Contacts

message connector supports Webex App contacts. message connector does nothing with Jabber contacts.

Note Existing contacts will not be transitioned across from Jabber to Webex.

Direct Messaging Interactions (One to One)

- All Hybrid Message users can use Webex App to send messages to all Webex App users in their organization.
- All Hybrid Message users can use Jabber to send messages to all Webex App users in their organization.
- Webex App users who are not entitled for Hybrid Message cannot send messages to the Jabber clients of other users.
- If both parties are Hybrid Message users, they can see the full to/from conversation in both clients.
- "Is Typing" status is supported. The user interface shows an indicator to one user when the other user has read a conversation or recently sent a message. The indicator will last for 5 minutes, even for spaces where the user is inactive.
- Read receipts are supported. To users, this means that the unread messages count is synchronized between Jabber and Webex App.

- When the Webex App user deletes a message from the 1:1 space, the Jabber user is notified that "*Username* used Webex App to delete a previously posted message". The corresponding Jabber message is not deleted.
- Plain text only. Webex App markdown is not converted to Jabber rich text. Jabber rich text is not converted to Webex App markdown.
- Editing messages in Webex App is supported. When a Message Service user edits a message in Webex App, the original version of the message is deleted in Webex App. The Message Connector sends the edited message to Unified CM IM and Presence.

  The recipient on Jabber sees the edited message as a new message, they also receive a notification "*Username* used Webex App to delete a previously posted message." However, they can disregard the delete notification, as they still see the original version of the message in Jabber.

  Webex App doesn't tell the user that the original message is still visible in Jabber - even though the original message is no longer visible in Webex App.

Offline Storage

Offline storage affects one to one messaging interactions from Hybrid Message users.

The expected behavior, when a Hybrid Message-entitled Webex App user sends a message to another Webex App user, is for the sender's Jabber to also send that message to the recipient's Jabber. If the recipient is not using Jabber then, depending on the state of offline storage, one of the following will happen:

- Offline storage is enabled on IM and Presence Service: The message is stored and will be sent if the recipient signs in to Jabber.
- Offline storage is not enabled on IM and Presence Service: The message is discarded and the sender will see a "Message could not be delivered" error, if they are using versions before 12.5.

  In this case, the sender and recipient may both have seen that this message has been delivered, because they're using Webex App. This is expected behavior but it could confuse users.

Offline storage is governed by the *Suppress offline instant messaging* setting on IM and Presence Service.

Note There is a known issue with offline messaging. When a Message Service user comes back online in Webex, stored messages are replayed in Webex but they may be out of sequence. The same messages are replayed in sequence in the user's Jabber client.

Group Messaging

Not supported. Webex App spaces are not converted to Jabber group chats. Jabber group chats are not converted to Webex App spaces.

The following is a list of known behaviors when users try group messaging interoperability. Note that there is usually no indication of a problem, which could cause confusion for your users.

- When Jabber users are creating group chats, or inviting contacts to group chats, they will be able to browse and select from Webex App users who are entitled for Hybrid Message. However, when they try to add these contacts to the group chat, the Webex App users are not added. Jabber users are added to the group chat as normal. There is no UI feedback to indicate a problem.
- If a Jabber user, who is entitled for Hybrid Message, switches to using Webex App, that user is immediately removed from the active rosters in all group chats with other Jabber users.
- Webex App users can add any Webex App-only or Hybrid Message users to spaces. For Hybrid Message users who are using Jabber, there is no indication that they have been added to the Webex App space. The only indication of this problem is to the other users in the space; there will be no read receipts from the affected Hybrid Message users.
- If a Hybrid Message user was once using Jabber to participate in a persistent group chat, and then switches to use Webex for their messaging interactions, their Active status in Webex is translated to Available presence in the persistent group chat. The other Jabber users may assume that the user is following the conversation. However, if the apparently Available user doesn't open Jabber, they may never be aware of later posts in that persistent conversation.

Presence Translation

We have taken a minimal approach to presence translation, based on the premise that the Hybrid Message Service is a transitionary arrangement to facilitate migration from Jabber to Webex App. Our design does not account for users indefinitely using both clients, because the way Unified CM IM and Presence calculates the composed presence can result in Jabber users seeing unexpected presence status of their contacts.

Presence of Jabber client, as seen by Webex App user

Presence is not translated from Cisco Jabber to Webex App.

Note This limitation has a consequence on the Do Not Disturb behavior: when a user manually resets their Jabber presence from "Do Not Disturb" back to "Available", the corresponding Webex App status does not change. This is confusing because typically this action would reset the presence on all of the user's logged in clients/devices.

Presence of Webex App app, as seen by Jabber user

Partially supported from Webex App to Cisco Jabber.

How it works:

message connector polls Webex once every 10 minutes for all users' presence status. It submits this to Unified CM IM and Presence Service as *device presence* (meaning inferred by the device/client, as opposed to manually changed by the user).

This approach has predictable results if Hybrid Message Service users are using either Webex App or Jabber but, in a migration scenario, we expect people to be using both clients.

When a user has more than one client or device that submits device presence, IM and Presence Service gives priority to the most recent update for that user, and displays that presence to all the subscribing Jabber users.

Whenever a user manually changes their Jabber status, IM and Presence Service gives priority to the manual presence. In this case, the device presence - whether from Webex App or Jabber - is not shown to other Jabber users.

The following table lists some of the presence states that Jabber users could see when you have Hybrid Message Service users. This is a best effort at mapping the possible scenarios because we cannot exhaustively test all possible interactions that occur in your environment:

Presence of a user, as seen by another Jabber user	**How that presence was established by IM and Presence Service**
Available The contact's presence indicator is green.	• The contact is only using Jabber, and Jabber has determined that the user is **Available**. • The contact is using Jabber and Webex App, and Jabber has determined that the user is **Available**. IM and Presence Service received that presence update more recently than presence from the same user's Webex App app. • Jabber users do not see this presence for a user who is only using Webex App.
Available @ Webex The contact's presence indicator is green, and displays text "@ Webex".	• The contact is only using Webex App, and was **Active** on Webex App within the last 10 minutes. • The contact is using Jabber and Webex App, and was **Active** on Webex App within the last 10 minutes. IM and Presence Service received that presence update more recently than device presence from the same user's Jabber client. • Jabber users do not see this presence for a user who is only using Jabber.
Available with custom message	• The contact is only using Jabber, and has manually changed their presence status. • The contact is using Jabber and Webex App, and has manually changed their presence status in Jabber. IM and Presence Service prefers the manually edited presence from Jabber over the device presence update from the same user's Webex App app. • Jabber users do not see this presence for a user who is only using Webex App.
Away The contact's presence indicator is amber.	• The contact is only using Jabber, and Jabber has determined that the user is **Away**. • The contact is using Jabber and Webex App, and Jabber has determined that the user is **Away**. IM and Presence Service received that presence update more recently than presence from the same user's Webex App app. • Jabber users do not see this presence for a user who is only using Webex App.
Away @ Webex The contact's presence indicator is amber, and	• The contact is only using Webex App, and was Active more than 10 minutes ago, but within the last 72 hours. In Webex App this displays as, for example, "**Active 2 hours ago**" or "**Active yesterday**".

Presence of a user, as seen by another Jabber user	How that presence was established by IM and Presence Service
displays text "@ Webex".	• The contact is using Jabber and Webex App, and was Active on Webex App more recently than they were Available in Jabber. IM and Presence Service received the Webex App device presence more than 10 minutes ago but within the last 72 hours. Also, it received that presence update more recently than it received device presence from the same user's Jabber client. • Jabber users generally do not see this presence for other users who are only using Jabber. Note that users who are enabled for Hybrid Message Service, but are not actually using Webex App, still have their presence composed as if they were using Webex App. In most cases their Jabber presence takes precedence, but it is possible that they can show as Away "@ Webex"; for example, if they are out of office and their calendars are integrated with Cisco Webex. • Away @ Webex can also mean that the user is **Out of Office** in Webex App. Webex App shows an Airplane overlay on that user's profile picture. Out of Office status in Webex App is provided by integration with user calendars. If the user's Webex App app is not integrated with their calendar, there is no Out of Office status in Webex App. If a Webex App user is using Webex App while their calendar reports Out of Office, their Webex App status could change back to Active. This would correctly be translated to Available in that user's Jabber presence. • Webex App user is not sharing status (the **Show statuses** box is unchecked in Webex App settings). Webex App users can choose to hide their status, which also prevents them from seeing status of other Webex App users. A Jabber user always sees these buddies as Away. The Message Connector will never destroy the user's XMPP session while the user is in an Away state. If the user is not showing their status, their session will persist even if they have not used Webex App within the previous 72 hours.
Away with custom message	• The contact is only using Jabber, and has manually changed their presence status. • The contact is using Jabber and Webex App, and has manually changed their presence status in Jabber. IM and Presence Service prefers the manually edited presence from Jabber over the device presence update from the same user's Webex App app. • Jabber users do not see this presence for a user who is only using Webex App.
Do Not Disturb The contact's presence indicator is red.	This is a user level setting, which means that all the user's logged in clients/devices - including phones where applicable - have the "Do Not Disturb" status. • The contact is using Jabber and has manually changed status to **Do Not Disturb**.

Presence of a user, as seen by another Jabber user	How that presence was established by IM and Presence Service
	If the user is also using Webex App, their Webex App presence is unaffected because Message Connector does not translate presence from Jabber to Webex App. Also, IM and Presence Service always prefers the manual DND from Jabber over the device presence from Webex App. • The contact is using Webex App and has manually changed status to **Do not disturb:** for a period between *30 minutes* and *24 hours*. If a Webex App user has turned on "Do not disturb", then Webex App shows other Webex App users a crescent Moon overlay on that user's profile picture. • The contact is using both clients and has manually changed status to **Do not disturb:** for a period between *30 minutes* and *24 hours*. This status persists in both clients until the period expires in Webex App, or until the user changes it in Webex App. A user who is using both clients cannot reset their Do Not Disturb status by changing their presence in Jabber (they can use Webex App, or wait for the DND to expire in Webex App). This is because the Message Connector does not translate presence from Jabber to Webex App.
Offline The contact's presence indicator is gray.	The other user has not used Webex App or Jabber within the last 72 hours. The message connector destroys the XMPP session it was holding for the offline user's Webex App. You can see the count of inactive Hybrid Message users, on a particular message connector host, at **Applications** > **Hybrid Services** > **Message Service** > **Message Service Status**.

Read about Webex app availability:

- *Webex | See People's Availability* (https://help.webex.com/wghlt5)
- *Webex | Stop Sharing Your Status* (https://help.webex.com/nkzs6wl)

File Transfer

- Webex App users can share files with Jabber users. When a file is attached to a 1:1 space in Webex App, the Jabber user gets a link to that file.
- The Jabber user gets a message if the Webex App user deletes a file from the 1:1 space.
- A Jabber user cannot send files to Webex App users.

  When a Jabber user is communicating with a Webex App user, Jabber's file transfer and screen capture options are disabled.

However, if the IM and Presence Service has Managed File Transfer (MFT) enabled, the user's Jabber options for these features appear to be usable. In this case, if the Jabber user tries to send a file, the Webex app user receives a notification that a file has been sent in Jabber.

If the Webex user is not logged in to Jabber when the file is sent, they do not receive the file.

This behavior affects the recipient whether they are using Jabber on-premises (registered to IM and Presence), or Jabber registered to Webex.

Migration Considerations

If you're using Hybrid Message Service to gradually migrate your user base from Cisco Jabber to Webex, the following issues and mitigations may help your planning.

- **Admin-generated invitations to join Webex:** One requirement to make Hybrid Message Service work is to have all your Jabber users in Cisco Webex, imported by CSV or by Hybrid Directory Service. When you import users, they will all get invitations to start using Webex, which you may want to prevent. If your organization is SSO-enabled in Control Hub, you can suppress the email invite behavior before you import the users. See https://help.webex.com/article/g5ey83.

  Unfortunately, you cannot suppress these initial email invitations unless your organization is SSO-enabled.

  Suppressing the email invitations will help to mitigate unintended early access to Webex.

- **User-generated invitations to join Webex:** Cisco Webex normally invites users (by email) to start using the Webex app, if they are already in Cisco Webex but not yet using the app. When you enable Hybrid Message Service, this "self subscribe" behavior is automatically disabled for your organization.

  The reason we designed it this way is because whenever a Message Service user messages another Jabber user, Webex generates an email to invite the recipient to start using the Webex app. This amounts to spam for any Jabber user who is not yet using Webex.

- **Unintended early access to Webex:** One requirement to make Hybrid Message Service work is to have all your Jabber users in Cisco Webex, imported by CSV or by Hybrid Directory Service. You may not want these users to start using Webex just yet but, if they are synchronized with Directory Service and also have SSO enabled, there is no technical reason to prevent them from using the Webex app. This could lead to interoperability problems for those users who are not enabled for Hybrid Message Service.

  For example:

  - A Hybrid Message user, talking to another user in Webex, can only see their own half of the conversation when looking at it in Jabber. The other user will also appear to be Offline in Jabber (even though they are Active in Webex).
  - In the same scenario, if the Hybrid Message user tries to use Jabber to continue the conversation, the messages go to the other user in Webex, but that user's responses do not come back to Jabber.

  If you are following a migration plan that requires users to stay on Jabber, despite technically being able to use Webex, you may want to prevent client installations or advise your users of potential interoperability issues.

- **A user's Jabber ID (JID) is not the same as a user's Webex UID:** The Webex UID must be the user's email address but the Jabber ID does not have to be the email address, even though it looks like one.

Do not search for a user's JID when you are in Webex. Use the JID (or name) to search for users in the Jabber client. Use the email address (or name) to search for users in Webex.

- **Offline message suppression:** Users who start chatting to each other using Webex will still have access to Cisco Jabber. If a user is online with both clients, the Hybrid Message Service tries to deliver messages with both clients. If the recipient is offline in Jabber, the sender could receive misleading offline messages from IM and Presence service.

  To mitigate this issue:

  1. Sign in to Cisco Unified CM IM and Presence Administration and go to **Messaging** > **Settings**.
  2. Clear the box labeled **Suppress offline instant messaging** and click **Save**.

Note There is a known issue with offline messaging. When a Message Service user comes back online in Webex, stored messages are replayed in Webex but they may be out of sequence. The same messages are replayed in sequence in the user's Jabber client.

Message Flows and Security

We encrypt all instant messages that we transmit across the public internet using the Key Management Service (KMS). By default, Webex App customers use the KMS in the Webex cloud, but the Hybrid Message also supportsHybrid Data Security, which provides on-premises KMS.

Messages from Cisco Jabber to Webex App

1. The sender sends a message from the Jabber client. The message goes to IM and Presence Service, which sends on to the Jabber client of the recipient. This is the normal IM and Presence Service flow, which you can make secure if you want to (beyond the scope of this document).
2. If the recipient is a dual user, entitled for Hybrid Message, then the message may also go to the message connector on the Expressway.

   It will not go to message connector if the recipient has not recently been active on Webex App; to save processing and memory resources, we assume that the user will not answer in Webex App if they have not been active for more than 72 hours.

   You can choose to secure the connections between the IM and Presence Service cluster and the Expressway cluster hosting the message connector.
3. The message connector interacts with the Key Management Service (via the cloud-based messaging service) to request an encryption key. The messaging service retrieves the key for an existing space, or a new key if this is the first message for a new space (aka "conversation" or "room"), and passes the key back to the message connector.
4. The message connector creates a new conversation in Webex, if necessary, and posts the encrypted message to that conversation.

   This encryption is not optional and requires no configuration.

5. Webex securely sends the message to the recipient's Webex App client. Description of the mechanism is beyond the scope of this document.

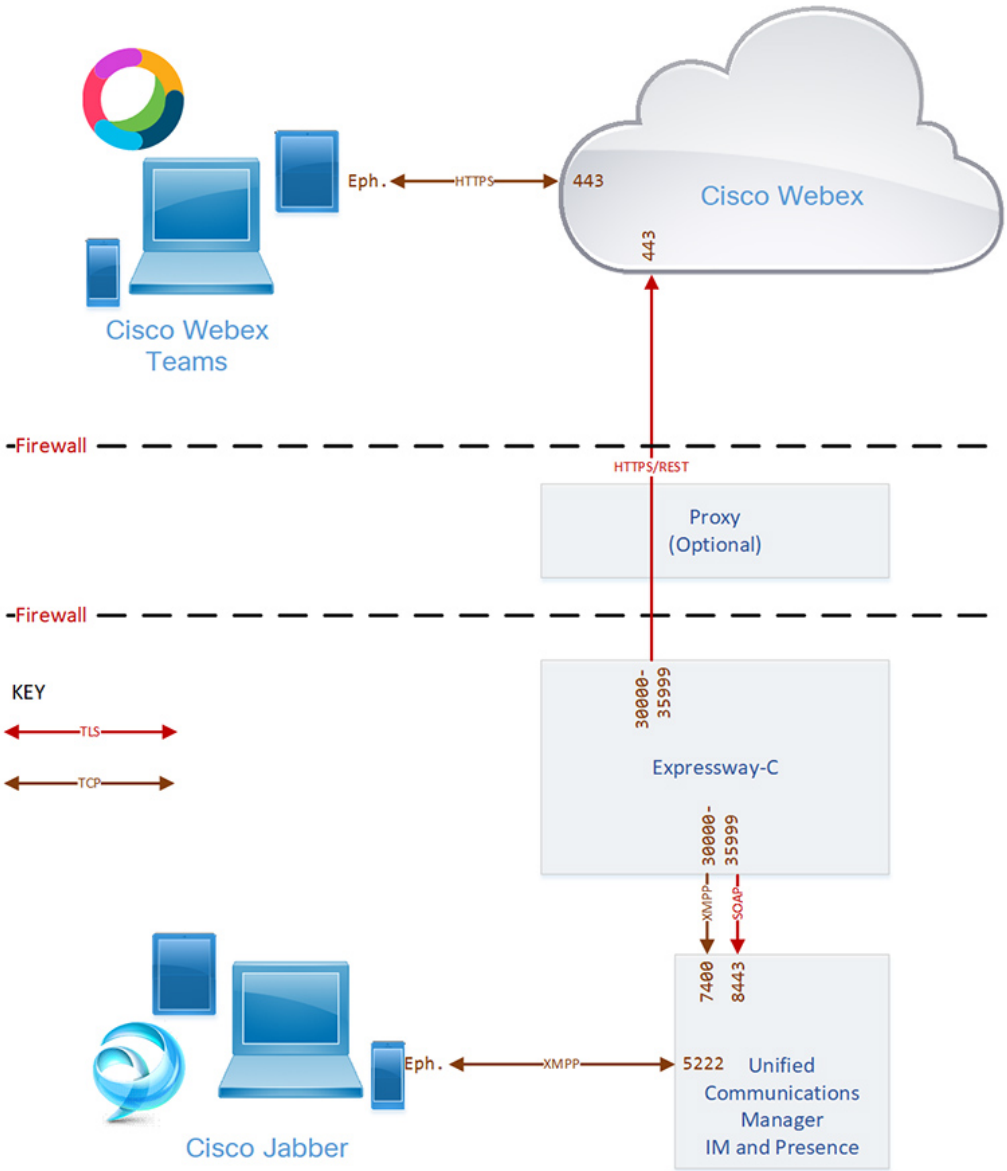
Messages from Webex App to Cisco Jabber

The Webex App app connects to Webex which provides a server certificate to authenticate itself. The app maintains this connection while the user is active. The app interacts with the Key Management Service to dynamically generate encryption keys for each user and each space (aka "conversation" or "room").

1. The sender uses Webex App to message the recipient. The Webex App app encrypts the message and sends it to Webex. Webex makes the encrypted message available to the recipient's Webex App client. This is the normal Webex App message flow; it is always secure, but description of the mechanism is beyond the scope of this document.
2. The Webex cloud checks its messaging service database to see if the sender and recipient are entitled to use Hybrid Message, and where to route the message towards the recipient.
3. The Webex cloud sends the encrypted message to the message connector.
4. The message connector interacts with the Key Management Service (via the cloud-based messaging service) to request the decryption key for the Webex App space.
5. The message connector decrypts the message and sends it to IM and Presence Service.
6. IM and Presence Service tries to route the message onwards to the Jabber client of the recipient.
7. When the message is read, the connector detects the read receipt and sends it back to Webex, so that the users' unread messages are consistent across their messaging clients.

Hybrid Message Connections

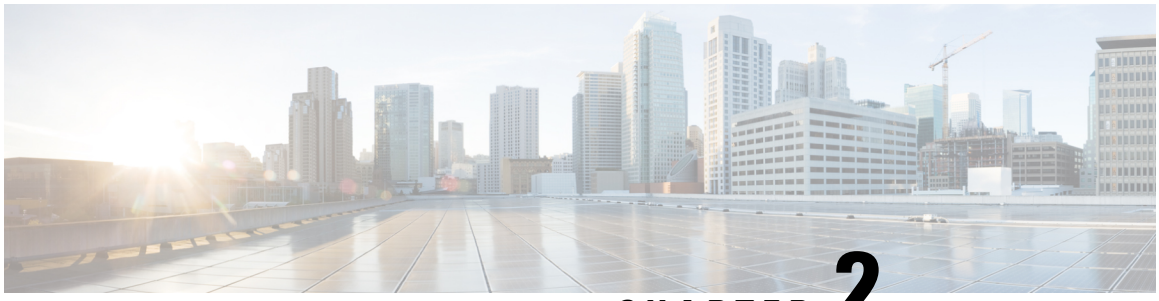
Figure 11: Hybrid Message Connections



Message Service Ports

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
Basic messaging	Webex App clients	Ephemeral	TCP	Webex hosts	443

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
Persistent HTTPS registration	Connector host Expressway	30000-35999	TLS	Webex hosts	443
XMPP (IM and Presence)	Connector host Expressway	30000-35999	TCP	Unified CM IM and Presence publisher	7400
AXL queries (Administrative XML Layer)	Connector host Expressway	30000-35999	TCP	Unified CM IM and Presence publisher	8443
Messaging and Presence	Cisco Jabber clients	Ephemeral	TCP	Unified CM IM and Presence publisher	5222



CHAPTER 2

Prepare Your Environment for Hybrid Message

Requirements for Hybrid Message

To enable Hybrid Message, you must use supported Cisco presence software listed in the table. Cisco Business Edition has Unified Communications Manager and IM and Presence Service as part of all of its packages, so make sure you have the right version.

Table 1: Required Cisco Components

Product Name	Version
Unified Communications Manager and IM and Presence Service (on-premises or service provider hosted)	11.5(1)SU3 or later • All publisher nodes must be running the AXL service. We also recommend, for HA deployments, that you run the AXL service on *all* nodes in the IM and Presence Service cluster. • If you have multiple IM and Presence Service clusters, you must have the Intercluster Sync Agent (ICSA) working across them. • If any of your IM and Presence Service clusters have been upgraded from a version earlier than 10.5(2), you must apply a Cisco Options Package (COP file) to those clusters, to prepare them for Hybrid Message. You can get the file *ciscocm.cup-CSCvi79393-v1.cop.sgn*, and instructions for applying it, from https://software.cisco.com/download/home/286269517/type/282074312/release/UTILS. • Your IM and Presence Service clusters must have Multiple Device Messaging (MDM) enabled (this feature is enabled by default).
Cisco Jabber (any client platform)	11.9 or later
Webex app (any client platform)	

You must be licensed to use Cisco Webex, so you can create your organization using Control Hub.

Table 2: Cisco Webex licensing

Product	SKU
Cisco Webex	Any cloud paid offer

You need to use the following systems to deploy and manage your Hybrid Message. These are more generally required when you deploy Webex App and Hybrid Services, not only for Hybrid Message.

Table 3: Supporting Systems

System	Why you need it
Control Hub	Log in to create your organization in Webex, then subsequently to manage your services, resources, and users. See https://collaborationhelp.cisco.com/article/nkp3vu5.
Directory Connector	[Optional] Map user attributes from your on-premises directory into Control Hub, so you can grant them ability to use Hybrid Services. See https://www.cisco.com/go/hybrid-services-directory
Cisco Unified CM Administration	Manually create users, or integrate with your on-premises directory to provision users for IM and Presence Service.
Firewalls	Open the required ports on firewalls between the component systems.

You must deploy Expressway to host the connectors. Organizations using Cisco Hosted Collaboration Solution do not need Cisco Expressway on their premises. Instead, their Hosted Collaboration Solution partner will deploy it in the cloud as part of their Hybrid Services offering.

Table 4: Cisco Expressway Details

Requirements	Version
Cisco Expressway Connector Host	You can download the software image from software.cisco.com at no charge. We recommend the latest released version of Expressway for connector host purposes. See *Expressway Connector Host Support for Cisco Webex Hybrid Services* (https://collaborationhelp.cisco.com/article/ruyceab) for more information.

Managing Users for Hybrid Message

On-premises User Population

Before you connect your Jabber deployment to Webex, your Jabber users may exist in the following places:

- **Cisco Unified CM Administration**

  This requirement is already fulfilled by having an on-premises deployment of Jabber. The Jabber users are unable to message each other if they do not exist in Unified CM.

Users can be created manually or synchronized with your LDAP directory.

- [Preferred] **LDAP directory**

  If you manage your users with an LDAP directory, then we recommend that you synchronize users to Unified CM Administration. The alternative is that you have two places to manage users, with manual synchronization.

  See the documentation for your version of IM and Presence Service at https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/tsd-products-support-series-home.html.

Cloud-based User Population

As part of deploying Hybrid Message, you must have a user population in your organization in Webex. If you have deployed other Hybrid Services, or Webex App, you should already have an organization and users in Webex.

We recommend that you import all your Jabber users to Webex, to maximize interoperability. These users do not need paid subscriptions, but they do need to have the "Message Free" entitlement for Webex. There are two ways to grant this entitlement, depending on whether you have paid subscriptions:

- If you have paid subscriptions available, enable the **Automatic License Assignment Template**, and Message Free entitlements will be assigned automatically by default.
- If you do not have paid subscriptions, add the users manually using CSV file import or Directory Synchronization, and Message Free entitlements will be assigned automatically by default.

We recommend that you enable SSO for your organization (in Control Hub) before you import Jabber users (see https://help.webex.com/lfu88u). With an SSO-enabled org, you have the option to suppress email invitations to imported Jabber users, if you don't intend to give those users access to Webex (see https://help.webex.com/nqj88gt).

You can manage your user population the following ways:

- Manually, by entering users individually in Control Hub.
- By importing a list of users from a file (comma separated values, based on a Cisco-supplied template) using Control Hub.

  You can also use Control Hub to do an export-edit-import round trip with CSV files, and thus to bulk modify the users' service entitlements.
- [Preferred] By synchronizing your organization in Webex with your on-premises directory. This option is called Hybrid Directory Service.

  See *Ways to Add and Manage Users in Cisco Webex Control Hub* (https://help.webex.com/nj34yk2).

To summarize: your user details may exist in several places, but they must at least be in Webex and in Unified CM Administration. The attribute that uniquely identifies the users in all places is their email address.

Irrespective of how you create the user populations on-premises and in the cloud, **the users' email addresses must match in all places**.

Change a Users Email Address

Administrators have the functionality in Control Hub to make changes to a users' email address.

1. Sign in to `https://admin.webex.com`
2. Click **Users** and then click a username to open that users' configuration.

3. Update the users' email address.

Note Ensure you update the users' mail id in Cisco Unified CM to match the new email address in Control Hub. It can take up to 10 minutes for message connector to pick up the user mail id change in Unified CM.

4. Click **Reactivate User**. Activation can take up to 10 minutes.

Suppress Admin Invite Emails

As part of your Message Service deployment, we recommend importing all your Jabber users into Control Hub. This action would normally generate email messages to those Jabber users, inviting them to start using Webex. You may not want all your Jabber users to start using Webex, because they may experience interoperability issues, so we recommend that you suppress those emails.

You should do this task *before* you bulk import users, or synchronize your directory with Control Hub:

Before you begin

Enable SSO for your Webex organization. See https://collaborationhelp.cisco.com/article/lfu88u. Without SSO, you cannot suppress invite emails. In that case, skip this task, but be aware that you will generate automatic email invites at a later stage in this process.

Procedure

Step 1 Sign in to Control Hub at https://admin.webex.com/login.

Step 2 Click **Settings** and find the **Email** section.

Step 3 Slide the **Suppress Admin Invite Emails** switch. See https://collaborationhelp.cisco.com/article/nqj88gt for detail.

What to do next

Complete the Expressway-C connector host prerequisites for Hybrid Services

Use this checklist to prepare an Expressway-C for Hybrid Services, before you register it to the Webex cloud to host hybrid services connector software.

Before you begin

We recommend that the Expressway-C be dedicated to hosting connectors for Hybrid Services. You can use the Expressway-C connector host for other purposes, but that can change the supported number of users.

Note As an administrator of hybrid services, you retain control over the software running on your on-premises equipment. You are responsible for all necessary security measures to protect your servers from physical and electronic attacks.

Procedure

Step 1 Obtain full organization administrator rights before you register any Expressways, and use these credentials when you access the customer view in Control Hub (https://admin.webex.com).

Step 2 Deploy the Expressway-C connector host in a cluster to account for redundancy. Follow the supported Expressway scalability recommendations:

- For Hybrid Message on a dedicated Expressway-C:
  - message connector can be hosted on multiple Expressway-C clusters of up to 6 nodes each.
  - message connector can be used with multiple Unified Communications Manager IM and Presence Service clusters.

Step 3 Follow these requirements for the Expressway-C connector host.

- Install the minimum supported Expressway software version. See the version support statement for more information.
- Install the virtual Expressway OVA file according to the *Cisco Expressway Virtual Machine Installation Guide*, after which you can access the user interface by browsing to its IP address. You can find the document in the list of Cisco Expressway Install and Upgrade Guides on cisco.com.

  Note The serial number of a virtual Expressway is based on the virtual machine's MAC address. The serial number is used to validate Expressway licenses and to identify Expressways that are registered to the Webex cloud. **Do not change the MAC address of the Expressway virtual machine when using VMware tools, or you risk losing service.**

- You do not require a release key, or an Expressway series key, to use the virtual Expressway-C for Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
- Use the Expressway web interface in a supported browser. (See the Cisco Expressway Administrator Guide.) The interface may or may not work in unsupported browsers. You must enable JavaScript and cookies to use the Expressway web interface.

Step 4 If this is your first time running Expressway, you get a first-time setup wizard to help you configure it for Hybrid Services.

Select **Webex Hybrid Services**. This ensures that you will not require a release key.

Step 5 Check that the following requirements are met for the Expressway-C connector host. You would normally do this during installation. See the *Cisco Expressway Basic Configuration Deployment Guide*, in the list of Cisco Expressway Configuration Guides on cisco.com, for details.

- Basic IP configuration (**System > Network interfaces > IP**)
- System name (**System > Administration settings**)

- DNS settings (**System > DNS**)
- NTP settings (**System > Time**)
- New password for admin account (**Users > Administrator accounts**, click **Admin** user then **Change password** link)
- New password for root account (Log on to CLI as root and run the passwd command)

Note Expressway-C connector hosts do not support dual NIC deployments.

Step 6 Configure the Expressway-C as a "cluster of one":

- We recommend that you configure the Expressway as a primary peer before you register it, even if you do not currently intend to install an extra peer.

  Caution When you change clustering settings on X8.11 and later, be aware that removing all peer addresses from the **System** > **Clustering** page signals to the Expressway that you want to remove it from the cluster. **This causes the Expressway to factory reset itself on its next restart.** If you want to remove all peers but keep configuration on the remaining Expressway, leave its address on the clustering page and make it the primary in a "cluster of one".

- Here are the minimum clustering settings required, but the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* has more detail:
  - Enable H.323 protocol. On **Configuration** > **Protocols** > **H.323** page, set **H.323 Mode** to On.

    H.323 mode is required for clustering, even if the Expressway does not process H.323 calls.

    Note You may not see the **H.323** menu item if you used the Service Select wizard to configure the Expressway for Hybrid Services. You can work around this problem by signing in to the Expressway console and issuing the command `xconfig H323 Mode: "On"`.

  - **System** > **Clustering** > **Cluster name** should be an FQDN.

    Typically this FQDN is mapped by an SRV record in DNS that resolves to A/AAAA records for the cluster peers.

  - **System** > **Clustering** > **Configuration primary** should be 1.
  - **System** > **Clustering** > **TLS verification mode** should be Permissive, at least until you add a second peer.

    Select Enforce if you want cluster peers to validate each others' certificates before allowing intercluster communications.

  - **System** > **Clustering** > **Cluster IP version** should match the type of IP address of this Expressway-C.
  - **System** > **Clustering** > **Peer 1 address** should be the IP address or FQDN of this Expressway

    Each peer FQDN must match that Expressway's certificate if you are enforcing TLS verification.

Caution To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.

Step 7 If you have not already done so, open required ports on your firewall.

- All traffic between Expressway-C and the Webex cloud is HTTPS or secure web sockets.

- TCP port 443 must be open outbound from the Expressway-C. See https://collaborationhelp.cisco.com/article/WBX000028782 for details of the cloud domains that are requested by the Expressway-C.

Step 8 Get the details of your HTTP proxy (address, port) if your organization uses one to access the internet. You'll also need a username and password for the proxy if it requires basic authentication. The Expressway cannot use other methods to authenticate with the proxy.

- We tested and verified Squid 3.1.19 on Ubuntu 12.04.5.
- We have not tested auth-based proxies.

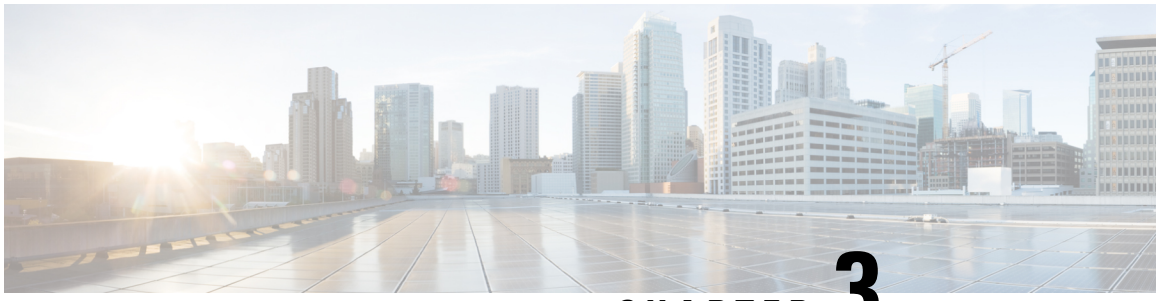
Note If your organization uses a TLS proxy, the Expressway-C must trust the TLS proxy. The proxy's CA root certificate must be in the trust store of the Expressway. You can check if you need to add it at **Maintenance** > **Security** > **Trusted CA certificate** .

Note The details of the proxy, as configured on the primary Expressway in the connector host cluster, are shared throughout the Expressway cluster. You cannot configure different proxies for different nodes in the cluster.

Step 9 Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

- Hybrid Services requires a secure connection between Expressway-C and Webex.

  You can let Webex manage the root CA certificates for you. However, if you choose to manage them yourself, be aware of certificate authorities and trust chains; you must also be authorized to make changes to the Expressway-C trust list.



CHAPTER 3

Deploy Cisco Webex Hybrid Message Service

Register Expressway-C connector hosts to Cloud

Hybrid Services use software connectors hosted on Expressway-C to securely connect Webex to your organization's environment. Use this procedure to register Expressway-C resources to the cloud.

After you complete the registration steps, the connector software is automatically deployed on your on-premises Expressway-C.

Before you begin

- Make sure your Expressway-C is running on a version that's supported for hybrid services. See the *Supported Versions of Expressway for Cisco Webex Hybrid Services Connectors* documentation (https://help.webex.com/article/ruyceab) for more information about which versions are supported for new and existing registrations to the cloud.
- Sign out of any open connections to the Expressway-C interface that are open in other browser tabs.
- If your on-premises environment proxies the outbound traffic, you must first enter the details of the proxy server on **Applications > Hybrid Services > Connector Proxy** before you complete this procedure. Doing so is necessary for successful registration.

Procedure

Step 1 Sign in to the customer view of https://admin.webex.com/login.

Step 2 In the left-hand navigation pane, under **Services** click **Hybrid** and then choose one:

- If this is the first connector host you're registering, click **Set up** on the card for the hybrid service you're deploying, and then click **Next**.
- If you've already registered one or more connector hosts, click **View all** on the card for the hybrid service you're deploying, and then click **Add Resource**.

The Webex cloud rejects any attempt at registration from the Expressway web interface. You must first register your Expressway through Control Hub, because the Control Hub needs to hand out a token to the Expressway to establish trust between premises and cloud, and complete the secure registration.

Step 3 Choose a method to register the Expressway-C:

- **New Expressways**—choose **Register a new Expressway with its Fully Qualified Domain Name (FQDN)**, enter your Expressway-C IP address or fully qualified domain name (FQDN) so that Webex creates a record of that Expressway-C and establishes trust, and then click **Next**. You can also enter a display name to identify the resource in Control Hub.

  Caution To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.

- **Existing Expressways**—choose **Select an existing Expressway cluster to add resources to this service**, and then choose the node or cluster from the drop-down that you previously registered. You can use it to run more than one hybrid service.

Tip If you're registering a cluster, register the primary peer. You don't need to register any other peers, because they register automatically when the primary registers. If you start with one node set up as a primary, subsequent additions do not require a system reboot.

Step 4 Click **Next**, and for new registrations, click the link to open your Expressway-C. You can then sign in to load the **Connector Management** window.

Step 5 Decide how you want to update the Expressway-C trust list:

A check box on the welcome page determines whether you will manually append the required CA certificates to the Expressway-C trust list, or whether you allow Webex to add those certificates for you.

Choose one of the following options:

- Check the box if you want Webex to add the required CA certificates to the Expressway-C trust list.

  When you register, the root certificates for the authorities that signed the Webex cloud certificates are installed automatically on the Expressway-C. This means that the Expressway-C should automatically trust the certificates and be able to set up the secure connection.

  Note If you change your mind, you can use the **Connector Management** window to remove the Webex cloud CA root certificates and manually install root certificates.

- Uncheck the box if you want to manually update the Expressway-C trust list. See the Expressway-C online help for the procedure.

  Caution When you register, you will get certificate trust errors if the trust list does not currently have the correct CA certificates. See Certificate Authorities for Hybrid Services, on page 35.

Step 6 Click **Register**. After you're redirected to Control Hub, read the on-screen text to confirm that Webex identified the correct Expressway-C.

Step 7 After you verify the information, click **Allow** to register the Expressway-C for Hybrid Services.

- Registration can take up to 5 minutes depending on the configuration of the Expressway and whether it's a first-time registration.
- After the Expressway-C registers successfully, the Hybrid Services window on the Expressway-C shows the connectors downloading and installing. The management connector automatically upgrades itself if there is a newer version available, and then installs any other connectors that you selected for the Expressway-C connector host.
- Each connector installs the interface pages that you need to configure and activate that connector.

  This process can take a few minutes. When the connectors are installed, you can see new menu items on the **Applications > Hybrid Services** menu on your Expressway-C connector host.

Troubleshooting Tips

If registration fails and your on-premises environment proxies the outbound traffic, review the Before You Begin section of this procedure. If the registration process times out or fails (for example, you must fix certificate errors or enter proxy details), you can restart registration in Control Hub.

Certificate Authorities for Hybrid Services

The table lists the Certificate Authorities that your on-premises or existing environment must trust when using Hybrid Services.

If you opted to have Webex manage the required certificates, then you do not need to manually append CA certificates to the Expressway-C trust list.

Note The issuers used to sign the Webex host certificates may change in future, and the table below may then be inaccurate. If you are manually managing the CA certificates, you must append the CA certificates of the issuing authorities that signed the currently valid certificates for the hosts listed below (and remove expired/revoked CA certificates).

Cloud hosts signed by this CA	Issuing CA	Must be trusted by	For this purpose
CDN	`O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root`	Expressway-C	To ensure Expressway downloads connectors from a trusted host
Common identity service	`O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority`	Windows Server 2003 or Windows Server 2008 hosting the Cisco directory connector Expressway-C	To synchronize users from your Active Directory with Webex and to authenticate Hybrid Services users

Cloud hosts signed by this CA	Issuing CA	Must be trusted by	For this purpose
Webex App	`O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority`	Expressway-C	

Related Topics

Supported Certificate Authorities for Cisco Webex

Configure an Application Account for Message Connector

Configure an account for Message Connector to access the AXL API of the Unified Communications Manager IM and Presence Service. **You must use an independent administrator account, not the main administrator account**. Remember the details of this account so you can enter them in the Message Connector configuration later.

Procedure

Step 1 From Cisco Unified CM Administration, go to **User Management** > **Application User**, and then choose one:

- Click **Find** and, from the list, choose the administrator account that the connector will use to communicate with Unified Communications ManagerIM and Presence Service.
- Click **Add New** to create a new application user account.

Step 2 Configure the account with the **Standard AXL API Access** role.

Step 3 Click **Save**.

Configure the Connection to IM and Presence Service

To enable Hybrid Message , you must link Message Connector to your IM and Presence Service cluster by entering server information for the publisher node. This step builds a bridge between IM and Presence Service and the Webex cloud, with the connector acting as a broker between the two.

On each Expressway cluster that you are using for Hybrid Message , sign in to the primary node and complete the following configuration:

Before you begin

- Configure an Application Account for Message Connector, on page 36
- The connector on Expressway maintains a resilient connection between your Hybrid Message cluster and the cloud. You only need to add the publisher to the Expressway-C connector configuration. If a specific node goes down in the cluster, the connector will move to another server.

Procedure

Step 1 Go to **Applications** > **Hybrid Services** > **Message Service** > **Message Service Configuration**

Step 2 Click **New**.

Step 3 Enter the hostname or IP address of the IM and Presence Service publisher node that has Cisco AXL Web Service enabled.

The connector uses AXL to query the publisher and discover the other nodes in the cluster.

Step 4 Enter the credentials of the message connector AXL account you created on the IM and Presence Service publisher.

Note This must not be the main administrator account. You must create an account explicitly for the Message Connector.

Step 5 (Optional) Change **Certificate validation** to **Disabled** if you want Expressway to waive the check on the server certificate from the publisher node.

If certificate validation is enabled (which is the default), then the tomcat certificate from the IM and Presence Service node must be valid and signed by a CA that the Expressway trusts. If you are using a self-signed certificate, copy it into the Expressway's *Trusted CA certificate* list.

Step 6 Click **Add** to store the connector configuration on the Expressway-C.

Step 7 Repeat this task if you need to connect this Expressway cluster to any other IM and Presence Service clusters.

What to do next

Start the message connector, on page 37

Start the message connector

Manually enable the message connector after you configured the connector with the IM and Presence publisher and the AXL account.

Procedure

Step 1 From Expressway-C, go to **Applications > Hybrid Services > Connector Management**, and then click **Message Connector**.

Step 2 Choose **Enabled** from the **Active** drop-down list.

Step 3 Click **Save**.

The connector starts and the status changes to **Running** on the **Connector Management** window.

Verify the Connector Status

Verify that the message connector is running, before you enable users for Hybrid Message .

Procedure

From Expressway-C, go to **Applications** > **Hybrid Services** > **Message Service** > **Message Service Status**. Verify the configuration items in the **Status** column.

What to do next

Enable Hybrid Message for Users, on page 38

Enable Hybrid Message for Users

Use this procedure to enable Webex App users one at a time for Hybrid Message .

See *Ways to Add and Manage Users in Your Organization* (https://help.webex.com/nj34yk2) for other methods, such as using a bulk CSV template or Active Directory synchronization through Cisco directory connector.

Note When you use bulk import or directory synchronization to import users, users must have email addresses in the source system. Those must be the addresses they use for Webex App because you map them to the Webex user ID.

If a user does not have an email address in IM and Presence Service, the message connector cannot discover the user. Hybrid Message does not work for that user.

Using Cisco Directory Connector you can map a chosen attribute (eg. the mail attribute or the userPrincipalName attribute) to the Webex UID, but **the value of the attribute must be the user's email address**.

Procedure

Step 1 Sign in to https://admin.webex.com, go to **Users**, choose a specific user from the list, or use the search to narrow the list, and then click the row to open an overview of the user.

Step 2 Click **Edit**, and then ensure that the user is assigned at least one paid service under **Licensed Collaboration Services**. Make necessary changes, and then click **Save**.

Step 3 Open the **Hybrid Services** tab, and toggle on **Message Service** then save.

The user experiences a delay of up to one hour before reliably being able to send messages from Webex to Jabber.

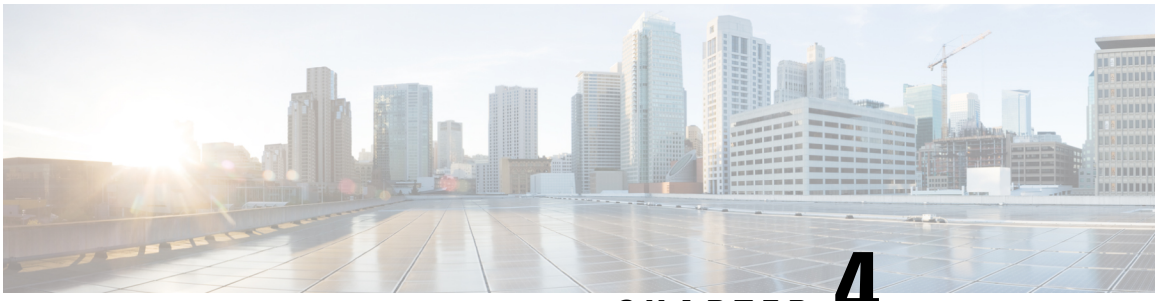
Test Hybrid Message

Before you begin

You need at least two users who are enabled for Hybrid Message. They should both have Cisco Jabber and Webex App installed.

Procedure

	Command or Action	Purpose
Step 1	One user opens Webex App client.	Let's call this person user A or Alice for the sake of this procedure.
Step 2	The other user opens Cisco Jabber client.	Let's call this person user B or Bob for the sake of this procedure.
Step 3	Send a message from Alice's Webex App client to Bob's Jabber client.	
Step 4	Check that the message arrives in Bob's Jabber client and that Alice's status shows there as "Available".	
Step 5	Reply from Bob's Jabber client to Alice's Webex App client.	
Step 6	Check in Alice's Webex App client that Bob appears to be typing.	
Step 7	Repeat the test, starting from Alice's Jabber client and Bob's Webex App client.	



CHAPTER 4

Manage Hybrid Message Service

Hybrid Message Status on Expressway

Each Expressway connector host enables part of your Hybrid Message deployment and shows status information about that part only. This is useful if you already know that a specific Expressway is affected by, or responsible for, an issue.

If you are looking for a more general overview of your service status, open your Hybrid Message deployment in Control Hub.

The status information page is at **Applications** > **Hybrid Services** > **Message Service** > **Message Service Status**. The information shown there falls into the following categories:

- Connectivity to Webex
- User and usage stats
- Connections to IM and Presence Service infrastructure

The status page and this reference topic are ordered by the level of impact that the status item will have on your service.

Connectivity to Webex

If this status is anything other than "Operational", then there is a problem between this Expressway and Webex. It could be a problem with the Expressway (check **Status** > **Alarms**), the service (check status.webex.com), or the network between them (check the proxy if you have one, check firewalls allow outbound HTTPS connections, use network diagnostic tools to establish if routes exist).

Message Service User Totals (this Expressway)

This part of the status page is about the total user populations known to this Expressway cluster. The numbers are common across this connector host cluster, because all nodes in the cluster share the Hybrid Message configuration (where you entered the publisher address and account details).

Users from connected IM and Presence clusters is the count of users that the connector gathers from the directly connected IM and Presence Service infrastructure. These users are "homed" on (or "local" to) the IM and Presence clusters whose publishers' details you entered on this Expressway cluster's primary node.

We need to distinguish this number because, when the connector makes AXL queries to those publishers, the publishers return all the users they know about. This includes 'intercluster' users, which the queried publishers know about because ICSA (Intercluster Sync Agent) is working across multiple IM and Presence clusters.

This number is the theoretical maximum of users that you could have using the service through this connector host cluster. In practice, you would probably enable a smaller subset of these, as part of a migration plan.

Users from all IM and Presence clusters (ICSA) is the count of users known to all IM and Presence clusters that are synchronized (by ICSA) with the publishers you added to the connector configuration. The number includes the count of local users (the previous number in this section). So, when you read the two numbers, you can think of them as, for example, 300 **of** 1000, if 300 users are homed on the directly connected IM and Presence clusters and 1000 are synchronized between multiple IM and Presence clusters.

You can use the relationship between these numbers to help validate or troubleshoot your Message Service deployment. For example, if you know you should have 1000 synchronized users but the total is less, you may have an intercluster sync agent problem. If you only have one cluster, or if all the IM and Presence publishers are configured on this connector, then the two numbers should be the same. If both numbers are 0, it could indicate an AXL query problem or a message connector configuration problem.

Users Enabled for Hybrid Message Service is the number of Hybrid Message-enabled users that Webex has assigned to this particular Expressway cluster. It is typically smaller than **Users from connected IM and Presence clusters**.

When you grant the message service to your users in Control Hub, the cloud communicates with the connector hosts to determine which connectors know about those users. The cloud then assigns those users to those connectors in a balanced way.

Active Message Service Users is the count of enabled users that are currently using the Hybrid Message. Users are considered Active if, within the 72 hours leading up to now, they have used Webex App to read or write messages to or from Cisco Jabber. It is also shown as a percentage of Users Enabled for Hybrid Message Service.

Users not Active for 72 Hours or more is the count of enabled users that are not currently using the Hybrid Message. Within the rolling 72 hour period up to now, these users did not use Webex App to read or write messages to or from Jabber. The connector uses this characteristic to improve performance, by deleting any sessions that are held by inactive users. In typical usage across your deployment, you can expect there to be some inactive users (holiday etc.) but the number should typically be lower than the Active users. It is also shown as a percentage of Users Enabled for Hybrid Message Service.

Message Service Status (IM and Presence Nodes)

This section of the page is about the connector's relationships with directly connected IM and Presence nodes.

For each IM and Presence publisher (the address you entered during configuration) there is at least one discovered node (itself) and there may be up to six in total.

The following status information is shown for each node in each IM and Presence Service cluster:

- **Node Version** is the IM and Presence Service software version, as reported by the particular node.
- **Node Status** should be "Operational". The "Outage" status indicates a problem with that IM and Presence Service node, or the connection to it.

- **Certificate validation** is either On or Off, depending on the choice you made when you connected to this node's publisher. If it's On (default), then the Expressway must be able to validate the certificate presented by this node, or the Hybrid Message will not work.
- **Message Service Users from this Node** is the count of Hybrid Message-enabled users who are assigned to this connector and are homed on this IM and Presence Service node. Each IM and Presence Service node that is listed on this status page contributes a portion to the total count of Users Enabled for Message Service, shown near the top of the page.
- **Active Message Service Users** is the count of enabled users that are currently using the Hybrid Message, and are homed on this IM and Presence Service node. Each IM and Presence Service node that is listed on this status page contributes a portion to the total count of Active Message Service Users, shown near the top of the page.
- **Users not Active for 72 Hours or more** is the count of enabled users that are not currently using the Hybrid Message, and are homed on this IM and Presence Service node. Each IM and Presence Service node that is listed on this status page contributes a portion to the total count of Users not Active for 72 Hours or more, shown near the top of the page.

High Availability and Failover

Controlled Outages of Message Connector Nodes

Before you start maintenance on an Expressway node that is hosting Message Connector, you should move the node into maintenance mode in *Control Hub*. This enables Cisco Webex to move the users off that node and onto the remaining nodes in the cluster, so that you can do your maintenance.

Cisco Webex does not recognize the Expressway's own maintenance mode. If you take an Expressway out of service in this way, it looks like an uncontrolled outage of that connector to Cisco Webex.

High Availability Setting on Presence Redundancy Groups

The Message Service connector is aware of the high availability setting. It can respond to manual or automatic failover and fallback events on the IM and Presence nodes.

If you change the group's high availability setting (either on or off) while the group's nodes are participating in Message Service, then you must restart the connector on the associated Expressway.

See https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-im-presence-service/200958-IM-and-Presence-Server-High-Availability.html for more on the IM and Presence configuration.

Controlled Outages of IM and Presence Service Nodes

Before you start maintenance on an IM and Presence Service node, you should manually failover the sessions from that node to the other node in the Presence Redundancy Group.

When you manually fail over one of the IM and Presence nodes in a Presence Redundancy Group, the user sessions from the source node migrate to the other node. The Expressway's Message Service status page reports "Outage" status for the source node, but shows users still assigned to that node.

The Message Connector is rate limited when creating new sessions on the target IM and Presence Service node. The connector could take up to 15 minutes to start transitioning users to the other node, and then

progresses at a rate that does not overwhelm the target node. For example, with 5,000 user sessions failing over, you can expect to wait approximately 30 minutes for the service to stabilize after the start of the controlled outage.

Wait until the transition process is complete, then you can do your maintenance on the IM and Presence Service node. Finally, you can manually fallback the sessions to the original node. You can expect a similar wait for the fallback to complete.

Uncontrolled Outages

The Hybrid Message Service automatically responds to an unexpected failure of an IM and Presence Service node.

As with the controlled outage, the Message Connector is rate limited when creating new sessions on the remaining IM and Presence Service node. The connector could take up to 15 minutes to start transitioning users to the other node, and then progresses at a rate that does not overwhelm the target node. For example, with 5,000 user sessions failing over, you can expect to wait approximately 30 minutes for the service to stabilize after an unexpected failure of one of the IM and Presence nodes.

The service is not robust to other uncontrolled outages, including but not limited to:

- Unexpected failure of an Expressway.
- Unexpected failure of Message Connector.
- Unexpected failure of the IM and Presence services that Hybrid Message Service depends on, including XCP, AXL, and the Presence Engine.

Refresh Connections to Unified CM IM and Presence Nodes

The Message Connector uses AXL calls to the IM and Presence publisher to discover the nodes in that cluster. This is a static arrangement and the Message Connector does not dynamically adapt when you change the IM and Presence cluster. For example, when you add or remove nodes.

The Message Connector cannot discover IM and Presence nodes when the AXL service is not running on the nodes. So, if there has been some kind of failure in your deployment, the nodes may not be back up before the Message Connector starts, or the AXL service may not have restarted.

When the Message Connector has not discovered some of the IM and Presence nodes, you can restart the Message Connector to force a rediscovery.

Procedure

Step 1 Sign in to the primary peer of the Message Connector Expressway cluster, and go to **Applications > Hybrid Services > Connector Management**.

Step 2 Click **Message Connector**.

Step 3 Choose **Disabled** from the **Active** drop-down list.

Step 4 Click **Save**.

The connector stops.

Step 5 Choose **Enabled** from the **Active** drop-down list.

Step 6 Click **Save**.

The connector starts and the status changes to **Running**.

Troubleshooting Hybrid Message

Webex Status

If all users are affected, the first thing you should check is whether the Hybrid Message is operational:

1. Browse to `https://status.ciscospark.com/`

   .
2. Expand **Webex Hybrid Services** > **Message Service** to read the status.

   If the Hybrid Message status is not Operational, we are trying to fix it.

Service Activation

Sign in to `https://admin.webex.com`

- Does your organization have the Hybrid Message card?

User Activation

Check Control Hub for user activation problems:

1. Sign in to `https://admin.webex.com`
2. Click **Users** and find the users you're interested in.

   You can sort the list by **Status**.
3. Click a username to open that user's configuration.

   If there is no **Message Service** link, you need to onboard the user for Hybrid Message.
4. Click **Message Service**.

   The slider should be on (to the right position). If it is not, slide it to on and save: the user status goes Pending for a few seconds and then Active.
5. If the user status is Error, review the message. Also, click **See history** to get more information about what is preventing this user's activation.
6. Correct the problem preventing activation, then come back to the user and click **Reactivate User**.

   If the user status is still not Active, you should raise a case.

Connector Status

If Hybrid Message is not working for all users, or a large subset, you should check the message connector status on Expressway:

1. Sign in to the primary peer of the cluster you registered and configured for Hybrid Message.
2. Go to **Applications** > **Hybrid Services** > **Connector Management**.
   - Is Management Connector running?
   - Is message connector running?
3. Go to **Applications** > **Hybrid Services** > **Message Service** > **Message Service Status**
4. Review the page for any errors between the Expressway and the configured IM and Presence Service nodes.

   Status should be *Operational*. There should be users assigned on-premises and subscribed to the cloud. If people are using Hybrid Message, then there should be some percentage of users with active sessions.

Check the IM and Presence Service node configuration on the Expressway:

1. On the Expressway, go to **Applications** > **Hybrid Services** > **Message Service** > **Message Service Configuration**.
2. Check the listed nodes. Are any of the status entries not **Active**?

Note There is a known issue where the software version of the IM and Presence node is not correctly synchronized on the Expressway after the IM and Presence node is upgraded. This is a purely cosmetic issue as the Message Connector does not use the version information for any purpose. You can synchronize the IM and Presence version by restarting the Message Connector. We intend to resolve this issue in a future Message Connector release.

3. Delete any affected nodes.
4. Recreate the nodes you deleted. Each time, make sure to correctly enter the address, username, and password, and then save the configuration.

   If the status does not improve, perhaps there is a configuration or connectivity issue on the IM and Presence Service nodes.

IM and Presence Service Checks

- Are the users you are investigating homed on the same IM and Presence Service cluster that is being used with Hybrid Message?
- Does the Message Connector account have the AXL role? Are the username and password of that account the same as what you entered on the Message Connector?
- Users are in Error state in Control Hub, with 'duplicate Mail ID' errors: These users are probably homed on more than one IM and Presence cluster. This situation could be a result of the way you import users to IM and Presence from Active Directory. Users should not be homed on multiple IM and Presence clusters. Run the IM And Presence troubleshooter to check for and correct any duplicate user accounts.
- Are the IM and Presence Service nodes running the Cisco AXL Web Service? Go to **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation** to check.

Per User Checks

If one or two users are affected, try the following checks:

- Is the user entitled for Hybrid Message?
- Did the user activation fail the first time? Open the user in Control Hub, open the Hybrid Message Service, and click **Reactivate User**.
- Does the user have an email address (mailid) in IM and Presence administration?
- Does the user's email address in IM and Presence match what is in Control Hub?
- Is there a new 'duplicate' Webex user named after the user's Jabber ID (JID)? This could result from searching for a JID in Webex. When you search for a JID, Webex may create a new space based on the JID, even though there is already an account based on the same user's email address.
- Did you use Directory Connector to import/synchronize users? Check that the LDAP attribute that you mapped to cloud *UID* contains the user's email address.

  For example, if you choose to map *UserPrincipalName* to cloud *UID*, then in Active Directory the UserPrincipalName attribute must contain the user's email address.
- Are the users correctly entitled in Cisco Webex? The 'Jabber only' users in your organization must be entitled to use the Message Free service with Webex, even though they are not using Webex, to ensure that they get messages sent via Webex by Message Service users.

  To avoid getting into this situation, we recommend that you assign the Message Free entitlement to all users. You can do this by configuring an Automatic License Assignment Template in Control Hub *before you import users*.

  If you already have many users in Control Hub who do not have the correct entitlement, you can resolve the situation by exporting all users to a CSV file, and then reimporting all the users from the CSV file. This works because importing users by CSV automatically applies the Message Free entitlement. Importing users with Hybrid Directory Service does not automatically apply this entitlement unless you use an automatic license assignment template.

  For a small number of affected users, you may prefer to manually apply their entitlement - especially if you have a diverse set of entitlements in your user population.
- Are Message Service users losing messages in Jabber? When a Message Service user hides their status in Webex (the **Show status** setting is unchecked), then that user's presence is reflected as "Away" in Jabber. However, the Message Service continues working for that user, and processes their messages from IM and Presence up to Webex. If the user is only using Jabber, but is not actually using the client while the messages are coming in, the message may not ever appear in Jabber as it does not persist messages. This could be mitigated by enabling offline storage in IM and Presence, but we recommend that users affected like this should check the Show status setting in Webex. They could also use Webex which persists the messages.

Hybrid Services Log

Note The Expressway's **Experimental** menu is not supported or documented.

You can read what the message connector is logging by reviewing the Hybrid Services Log on the Expressway:

1. Manually enter the URL for the /setaccess page, e.g. `https://<IPAddressOrFQDN>/setaccess`
2. Enter the value `qwertsys` in the **Access password** field then click **Enable access**.

   The **Experimental** menu is visible now.
3. Click **Experimental** > **Hybrid Services Log** > **Hybrid Services Log**.
4. Investigate the log for error conditions.

   If you are having a repeatable or persistent problem, you should raise a case. You may be advised to change the log levels or take a diagnostic log to send to Cisco (**Maintenance** > **Diagnostics**).

Proxy Server Updates

Whenever proxy settings are updated on **Applications** > **Hybrid Services** > **Connector Proxy** during runtime, a restart of hybrid services is required.