



Prepare Your Environment for Hybrid Message

- [Requirements for Hybrid Message, on page 1](#)
- [Managing Users for Hybrid Message, on page 2](#)
- [Suppress Admin Invite Emails, on page 4](#)
- [Complete the Expressway-C connector host prerequisites for Hybrid Services, on page 4](#)

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 <ul style="list-style-type: none"> • All publisher nodes must be running the AXL service. We also recommend, for HA deployments, that you run the AXL service on <i>all</i> 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 <i>ciscoem.cup-CSCvi79393-v1.cop.sgn</i>, 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 <i>Expressway Connector Host Support for Cisco Webex Hybrid Services</i> (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.

Complete the Expressway-C connector host prerequisites for Hybrid Services