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 3.

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 4
- 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 5

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 6

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.	