



# Deploy Expressway calendar connector for Microsoft Exchange

---

- Hybrid Calendar with Exchange deployment task flow, on page 1
- Configure a throttling policy for impersonation account , on page 3
- Register Expressway-C connector hosts to Cloud, on page 4
- Append the Exchange CA certificate to the Expressway trusted CA list, on page 6
- Link the calendar connector to Microsoft Exchange, on page 7
- Configure the Calendar Connector's Webex site settings, on page 9
- Choose how Hybrid Calendar localizes meeting join details, on page 10
- Configure @webex and @meet keywords, on page 11
- Customize email templates, on page 11
- Start the calendar connector, on page 13
- Enable Hybrid Calendar for users, on page 14
- Add Hybrid Calendar to workspaces with Webex room, desk, and board devices, on page 14
- Associate user's Personal Rooms with Webex, on page 15
- Test join button with room devices, on page 15

## Hybrid Calendar with Exchange deployment task flow

To deploy Hybrid Calendar with your Microsoft Exchange environment, perform the following tasks.

### Before you begin

[Prepare your environment](#)

### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<a href="#">Configure a throttling policy for impersonation account , on page 3</a>	A custom throttling policy helps the calendar connector work smoothly.
<b>Step 2</b>	<a href="#">Register Expressway-C connector hosts to Cloud</a>	Add the Hybrid Calendar to your organization and connect your Expressway to the Webex cloud. This creates a resource in

	<b>Command or Action</b>	<b>Purpose</b>
		<a href="https://admin.webex.com">https://admin.webex.com</a> and downloads connector software on to the Expressway.
<b>Step 3</b>	(Optional) <a href="#">Append the Exchange CA certificate to the Expressway trusted CA list, on page 6</a>	If you want Microsoft Exchange Web Services (EWS) traffic to be encrypted, make sure the Expressway trust list contains the certificate of the CA that signed the Exchange Server certificate.
<b>Step 4</b>	<a href="#">Link the calendar connector to Microsoft Exchange, on page 7</a>	Configure Exchange Servers for the calendar connector.
<b>Step 5</b>	(Optional) <a href="#">Configure the Calendar Connector's Webex site settings, on page 9</a>	If you have a Webex Meetings site, configure the @Webex functionality.
<b>Step 6</b>	(Optional) <a href="#">Choose how Hybrid Calendar localizes meeting join details, on page 10</a>	To override how the calendar connector localizes meeting join details for your entire organization, set the Default Language setting in <a href="https://admin.webex.com">https://admin.webex.com</a> .
<b>Step 7</b>	(Optional) <a href="#">Configure @webex and @meet keywords, on page 11</a>	To change the action that the calendar connector takes when users enter @webex or @meet, set the Keywords settings in <a href="https://admin.webex.com">https://admin.webex.com</a> .
<b>Step 8</b>	(Optional) <a href="#">Customize email templates, on page 11</a>	Choose what the Hybrid Calendar adds to meeting invitations, including audio or video join details and a localized header and footer in any language that the service supports.
<b>Step 9</b>	<a href="#">Start the calendar connector, on page 13</a>	
<b>Step 10</b>	<a href="#">Enable Hybrid Calendar for users, on page 14</a>	
<b>Step 11</b>	(Optional) <a href="#">Add Hybrid Calendar to workspaces with Webex room, desk, and board devices, on page 14</a>	If you want One Button to Push (OBTP) functionality to be provided to room and desk devices and Webex Boards that are registered to the Webex cloud, toggle on the calendar service for the device, and configure the room mailbox email address.
<b>Step 12</b>	(Optional) <a href="#">Associate user's Personal Rooms with Webex, on page 15</a>	For OBTP on Webex room and desk devices and Webex Boards, make sure that meeting schedulers have their Webex Personal Rooms associated with their Webex App accounts.
<b>Step 13</b>	<a href="#">Test join button with room devices, on page 15</a>	If you configured OBTP in the previous steps, test it with a device.

# Configure a throttling policy for impersonation account

A custom throttling policy helps the calendar connector work smoothly:

- The custom policy removes EWS limits from the impersonation account, to avoid issues such as maxconcurrency.
- The custom policy is tailored for an enterprise application. (The default policy is tailored for user load.)

## Before you begin

[Set Up an impersonation account for on-premises Microsoft Exchange](#)

This procedure is not required for Office 365.

## Procedure

---

**Step 1** In Exchange Management Shell, create the policy.

```
New-ThrottlingPolicy -Name "CalendarConnectorPolicy" -EWSMaxConcurrency unlimited  
-EWSMaxBurst unlimited -EWSRechargeRate unlimited -EWSCutOffBalance unlimited  
-EWSMaxSubscriptions 5000
```

**Step 2** If the impersonation account does not have a mailbox, run the following command:

```
Enable-Mailbox "impersonation account" -Database "database name"
```

**Step 3** Apply the new policy to the impersonation account:

```
Set-ThrottlingPolicyAssociation -Identity "impersonation account" -ThrottlingPolicy  
"CalendarConnectorPolicy"
```

where

- "**impersonation account**" is the name of the impersonation account you're using as the service account for the calendar connector.
- **CalendarConnectorPolicy** is the name of the policy that you created in Step 2.

**Step 4** Confirm that the mailbox is using the new policy:

```
Get-ThrottlingPolicyAssociation -Identity "impersonation account" | findstr  
"ThrottlingPolicy"
```

---

## What to do next

[Register Expressway-C connector hosts to Cloud, on page 4](#)

# 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 6](#).

**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.

# Append the Exchange CA certificate to the Expressway trusted CA list

If you want to verify the certificates presented by the Exchange Server, then the Expressway trust list must contain the certificate of the CA that signed the Exchange Server certificate. The CA certificate may already be in the trust list; use this procedure on each Expressway cluster to check the list and append the certificate if necessary.

If you're using a custom domain, make sure that you add the CA certificate for the domain certificate issuer to the Expressways.

## Before you begin

You must import certificates to each Expressway-C.

## Procedure

---

**Step 1** On the Expressway-C connector host, go to **Maintenance > Security certificates > Trusted CA certificate**.

**Step 2** Review the CA certificates in the trust list to check if the correct CA certificate is already trusted.

**Step 3** To append any new CA certificates:

- Click **Browse** (or the equivalent in your browser) to locate and select the PEM file.
- Click **Append CA certificate**.

The newly appended CA certificate appears in the list of CA certificates.

**Step 4** To replace an existing CA certificate with an updated one, for a particular issuer and subject:

- Check the check box next to the Issuer details.
  - Click **Delete**.
  - Append the replacement certificate as described above.
- 

# 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
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](#)

## Link the calendar connector to Microsoft Exchange

The calendar connector installs automatically after you register your Expressway connector host for Hybrid Services. The connector does not start automatically, and requires some configuration to link to your calendar environment.

**Procedure**

**Step 1** From the Expressway connector host, go to **Applications > Hybrid Services > Calendar Service > Microsoft Exchange Configuration**, and then click **New**.

**Note** Make sure you choose **Microsoft Exchange Configuration**, not **Cisco Conferencing Services Configuration**. You cannot configure the Calendar Connector for Microsoft Exchange or Office 365 in the same organization with the conferencing services (integration with Cisco TelePresence Management Suite).

**Step 2** Enter the credentials of the service account that you want the calendar connector to use to connect to Exchange. The service account queries calendars on behalf of your users, using the impersonation role. You can use these formats:

- **username@domain.com**—The userPrincipalName. Typically, this value matches the user's primary email address, but the properties are separate. userPrincipalName consists of the User Logon Name (not always the same as sAMAccountName) and the UPN suffix, which is based on the Active Directory domain (not always the same as the NetBIOS domain).

**Note** Use this format whenever possible.  
 If you used the simplified configuration with a single impersonation account to prepare a hybrid Exchange on-premises and Office 365 integration, you **must** use this format. Also, make sure that the impersonation account that you use is synchronized to the Office 365 cloud, and that its userPrincipalName matches one of the account's SMTP addresses.

- **DOMAIN\username**—DOMAIN is the NetBIOS domain (the pre-Windows 2000 domain); "username" is the sAMAccountName (the legacy username or pre-Windows 2000 username).

If you're unsure about what to use for these formats, use [Active Directory Users and Computers](#) on a Windows machine to view the Account tab of the Properties pane for the user in question. The correct values to use are displayed as:

- User logon name for the first format.
- User logon name (pre-Windows 2000) for the second format.

**Step 3** Enter a unique **Display Name** for this Exchange Server.

**Step 4** For the **Type**, select **Exchange On-Premises** for Exchange 2013, 2016, or 2019. (Select this type even if you are preparing a hybrid Exchange on-premises and Office 365 integration.)

**Step 5** For **Need Proxy for Connection?**, select **Yes** if https access goes through a web proxy to your Exchange environment.

**Step 6** For **Enable this Exchange server?**, select **Yes**.

You can select **No** for debugging purposes, but users will not be subscribed to this Exchange.

**Step 7** Check a value for the **Authentication Type**:

- For added security, we recommend **NTLM** for on-premises Exchange servers.
- For Hybrid Exchange (on-premises and Office 365) deployments, check both **NTLM** and **Basic** authentication types. If one method fails, then the other method is used.

**Step 8** Leave **TLS Verify Mode** as the default value (**On**) so that this Expressway-C verifies the certificate that the Exchange Server presents.

You may need to update the trust stores on both servers to ensure that each one trusts the CA that signed the other's certificate.

**Step 9** Under **Discovery**, select **Use Autodiscover** to enable autodiscovery. The calendar connector queries to find one or more Exchange servers.

**Note** You **must** use autodiscovery for deployments of Microsoft Exchange 2013 and later.

Use **Provide Exchange Address directly** only for troubleshooting or testing purposes. This option does not use autodiscovery. If you select it, enter the IPv4 address, IPv6, or FQDN of the Exchange server.

**Step 10** Configure the extra fields that are related to autodiscovery.

- Choose whether to **Enable SCP record lookup**.

If you set this field to **Yes**, the first autodiscover step that the calendar connector takes is an Active Directory Service Connection Point (SCP) record lookup to get a list of autodiscover URLs. The calendar connector uses the **Active Directory domain**, **Active Directory site**, **Query mode**, and **LDAP TLS Verify Mode** and fields only if you enable this step. These fields provide the information necessary to

find and query an LDAP server in Active Directory. Even if this step fails, autodiscovery may succeed at a later step.

- b) Enter the **Active Directory domain** to query for the SCP record.
- c) (Optional) Enter the **Active Directory site** that is geographically closest to the calendar connector, to optimize the query response time.
- d) Select a **Query mode** to control which directory access protocol that calendar connector uses to query Active Directory.

If you select **Idaps** (secure LDAP), the Domain Controller must authenticate itself by presenting a server certificate to this Expressway-C.

- e) Enable **LDAP TLS Verify Mode** if you want the Expressway-C to validate the certificate that the Domain Controller presents. This option checks the server name against the CN or SANs in the received certificate, and also checks that the issuing authority is in the local trusted CA list.
- f) Enter an **Email Address** so that calendar connector can test the autodiscover process (other than SCP record lookup, which uses the **Active Directory domain** instead).

Use the email address of a user that you will enable for the Hybrid Calendar Service, as it appears in Control Hub.

If the test fails, then your settings are not saved. If you omit the email address, then your settings are saved without verifying the autodiscover process (other than SCP record lookup, if enabled).

- g) (Optional) To manually configure any Autodiscover redirect URLs that the Calendar Connector should trust, click **Configure Trust List**.

Once you click **Add**, the Calendar Connector automatically populates any missing Autodiscover redirect URLs that it finds while contacting the Autodiscover service. URLs from unauthenticated sources are placed in pending state, and blocked unless you choose to allow them. If you skip this step now, you can still manually add URLs later, or explicitly accept or deny the pending URLs.

**Step 11** Click **Add** to store the Exchange Server configuration on the Expressway connector host.

The calendar connector tests the connection to the Exchange environment, and notifies you if there are pending Autodiscover redirect URLs to review.

**Step 12** (Optional) If your organization has multiple user email domains, we recommend that you test the autodiscover configuration with a user address from each email domain to ensure that the process works for all of them. To test another address, change the value of the **Email Address** field to a different address, and then click **Save..**.

---

#### What to do next

[Configure the Calendar Connector's Webex site settings, on page 9](#)

## Configure the Calendar Connector's Webex site settings

After you configure the Exchange settings, configure the details for your Webex Meetings sites. If you have more than one Webex site, do these steps for each site, and set the default to the site with the most users. Users who are not on the default site, or who want to use a different site, must [set up their Personal Room in the Webex app](#).

## Choose how Hybrid Calendar localizes meeting join details

### Before you begin

- For the @webex functionality to work for users, verify the following:
  - You have at least one Webex Meetings site, with the Personal Room feature enabled for the site and for the individual users.
  - The email address in each user's Webex account matches the user's Exchange email address and Webex App login address. If it does not, users must [set up their Personal Room in the Webex app](#).
- Gather the Webex user account email address of a valid user on your site. The calendar connector uses this account to access the Webex Personal Room details for users who schedule meetings with @webex.

### Procedure

---

**Step 1** From the Expressway-C connector host, go to **Applications > Hybrid Services > Calendar Service > Cisco Conferencing Services Configuration**, and then click **New**.

**Step 2** Select **Type** as **Webex** under **Conferencing Services Type**.

**Step 3** Enter the **Fully Qualified Site Name** for this Webex Meetings site.

**Example:**

If your site is accessed as example-co.webex.com, you'd enter example-co.webex.com.

**Step 4** Enter a valid Webex user account email address, leave the password field blank, and then click **Test Connection** to validate the site information that you entered. If testing the connection fails, you can save the configuration with both the user name and password fields blank.

**Step 5** Indicate whether or not this site is the default.

The default site is used for @webex unless the user has a different site configured in their My Personal Room setting in the Webex App app (either because the user's [Webex site has been linked to Control Hub by an administrator](#), or because the user [configured the setting](#) with a different site).

**Step 6** Click **Save** to save the configuration.

---

## Choose how Hybrid Calendar localizes meeting join details

In Control Hub, the Default Language setting controls the language of the join details that the Hybrid Calendar adds to invitations. If you leave the setting at its default, the service uses the language from the **item.Culture** property of each meeting invitation. (Typically, the scheduler's operating system controls the value of **item.Culture**.)

To override choosing languages on a meeting-by-meeting basis from **item.Culture**, choose a specific language to use for join details for all meetings across your organization.

### 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**.
- Step 3** From the Hybrid Calendar card for Exchange, click **Edit settings**.
- Step 4** In the **Meeting Invitations** section, choose a language from the **Default Language** drop-down list, and click **Save**.  
After you save the change, the Hybrid Calendar uses the language you choose each time it adds join to details a meeting. It doesn't change the language for existing join details.

---

## Configure @webex and @meet keywords

By default, when users add **@webex** to a meeting location, the calendar service updates the meeting with their Webex Personal Room details. When users add **@meet**, by default the service updates the meeting with Webex App space details. As an administrator, you can change these default actions for either keyword.

Regardless of how you set these actions, power users can add the modifier **:space**, **:myroom** or **:onet ime** to specify the action for either keyword. For example, adding **@webex:space** causes the service to update the meeting with Webex App space details. As well, **@webex:onet ime** creates a one-time Webex meeting.

### 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**.

- Step 3** From the Hybrid Calendar card for your calendar environment, click **Edit settings**.

**Note** If you have the Hybrid Calendar set up for multiple calendar environments, you can access the keywords settings from multiple pages in Control Hub, but the values that you set apply to all environments.

The Hybrid Calendar (Microsoft 365) displays a list of tenants included in this organization.

- Step 4** Select the tenant to configure.

- Step 5** Click the **Settings** tab.

- Step 6** In the **Keywords** section, select the default action that you want for each keyword.

- Step 7** Click **Save**.
- 

## Customize email templates

Choose which meeting join details Hybrid Calendar includes in meeting invitations.

### 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 **Meeting**.

**Step 3** Locate the **Customize Meeting Join Details** section.

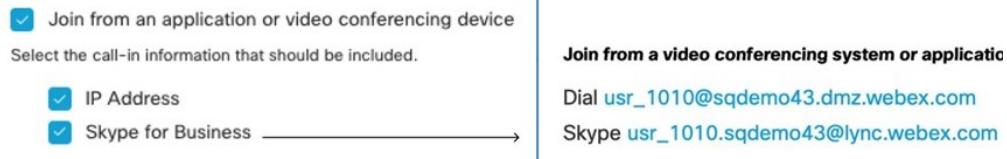
**Step 4** Choose whether to show **Join by Phone** details.

When you include the dial-in details, you can also choose to add a link to global call-in numbers, a link to toll-free calling restrictions, or both.



**Step 5** Show or hide details on joining from an application or video conferencing device.

When you include the video dialing details, you can also choose to include an IVR IP address, a Skype for Business join link, or both.



**Step 6** Click **Add a Language** and then select the language from the drop-down menu to create a custom header and footer for any of the languages that the Hybrid Calendar supports. When you've got the header and footer text that you want, click **Save**.

The header and footer values have a maximum of 1024 characters each (including spaces).

Localized header and footer

To edit the header and footer in each language, select the language in the dropdown, edit the header & footer for that language in the textboxes, and then click save.

The screenshot shows the Expressway interface for managing calendar connectors. On the left, there's a sidebar with a 'German' section containing 'Header Text' and 'Footer Text' fields. Below this are sections for 'English (United States)' and 'French'. A button 'Add a Language' is visible. At the bottom, a note says 'Use this language if nothing is defined for its header and footer.' with a dropdown set to 'French'. On the right, a large arrow points from the 'French' section towards the right panel. The right panel displays a meeting invitation for 'Wednesday, December 16, 2020 at 2:00 PM - 3:00 PM. @webex'. It includes options to 'Accept', 'Tentative', 'Decline', or 'Propose New Time'. Below this is a 'Please respond.' section with a note about not deleting or changing text. Further down are sections for 'Join meeting in my Webex Personal Room' (with a green 'Join' button) and 'Join by phone' (with a link to a US toll number). At the bottom, there's a note about joining from a video conferencing system or application.

- Step 7** Once you've added a custom header and footer for a language, you can choose that language as a default for any other language that doesn't have a custom header and footer defined. Your default language choice saves automatically.

## Start the calendar connector

You can do this task before you configure the calendar connector links to your Exchange environment and Webex environment, but all tests will fail until the calendar connector is **Running** and you may need to restart the connector after configuration.

### Procedure

- Step 1** From Expressway, go to **Applications > Hybrid Services > Connector Management**.

The **Connector management** section of the page has a list of connectors and the status of each. The **Management Connector** is **Running** and the **Calendar Connector** is **Not enabled**.

- Step 2** Click **Calendar Connector**.

- Step 3** Select **Enabled** from the **Active** drop-down list.

- Step 4** Click **Save**.

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

**What to do next**

[Enable Hybrid Calendar for users, on page 14](#)

## Enable Hybrid Calendar for users

Use this procedure to enable a small number of Webex users for Hybrid Calendar with Microsoft Exchange or Office 365.

See [Ways to add and manage users in Control Hub](#) for other methods, such as using a bulk CSV template or Active Directory synchronization through Cisco directory connector.

Any of these methods requires that users have signed in to the Webex App to be fully activated. To enable @webex for users who have never signed in to the app, add and verify the users' domain using the [Add, verify, and claim domains](#) process. (You must own a domain for it to be verifiable. You do not need to claim the domain.)

**Before you begin**

By default, users receive email notifications regarding the Hybrid Calendar, including a welcome email after you enable them. For steps to toggle off these **User Email Notifications**, see the [Configure notifications for Hybrid Services](#) help article.

**Procedure**

- 
- Step 1** Sign in to the customer view of <https://admin.webex.com/login>.
  - Step 2** In the left-hand navigation pane, under **Management** click **Users**.
  - Step 3** 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 4** 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 5** Click **Calendar Service**, toggle on **Calendar**, choose **Microsoft Exchange**, and then save your changes.  
After you activate the service, the user status changes from Pending Activation to Activated. The length of time for this change depends on the number of users that you're enabling for the service.  
If email notifications are enabled, users receive a message indicating that the feature is enabled.
- 

## Add Hybrid Calendar to workspaces with Webex room, desk, and board devices

**Before you begin**

This task assumes that you've already created places for the Webex room, desk, or board devices. If you need to create the workspace, see [Add shared devices and services to a workspace](#).

### Procedure

---

- Step 1** Sign in to the customer view of <https://admin.webex.com/login>.
- Step 2** In the left-hand navigation pane, under **Management** click **Workspaces** and select the workspace to modify.
- Step 3** Go to **Calendar** and click **Add Calendar** so that people can use One Button to Push (OBTP) from their Webex devices.
- Step 4** Select calendar service from the drop-down menu.
- Step 5** Enter or paste the email address of the room mailbox. (For help locating this email address, see "Create and manage room mailboxes" on the Microsoft Docs web site.)  
This is the email address that will be used to schedule meetings.
- Step 6** Click **Save**.
- 

## Associate user's Personal Rooms with Webex

To provide the join button to Webex room and desk devices and Webex Boards when scheduling Webex Personal Room meetings, users must have their Personal Room associated with their Webex App account. This can happen in one of the following ways:

- The users on your Webex site have been Webex App linked. (For site linking steps, see [Link Webex sites to Control Hub](#).)
- Users change their own preferred Webex site from the Webex App settings or preferences, see [Change your default meeting site](#)
- For a comprehensive approach, use the bulk CSV import process from Control Hub to set users' preferredWebExSite in the steps that follow.

### Procedure

---

- Step 1** Sign in to the customer view in <https://admin.webex.com>.
- Step 2** In the left-hand navigation pane, under **Management** click **Users**.
- Step 3** Click **Manage Users**.
- Step 4** See <https://help.webex.com/en-US/article/e2okky/Modify-Users-in-Control-Hub-with-the-CSV-Template> for the detailed CSV import/export procedure.
- Step 5** Use a CSV editor to change the **preferredWebExSite** attribute for all or some users.
- Step 6** Import the CSV file.
- 

## Test join button with room devices

Use these steps to set up a test meeting and verify OBTP on a registered device.

## Procedure

### Step 1

To test a Webex team meeting in Exchange or Office 365:

- a) In Outlook, Outlook Web Access, or <https://mail.office365.com>, create a new meeting, and then add a keyword such as **@webex:space** or **@meet** to the **Location** field.
- b) Go to the Scheduling Assistant and click **Add room**, and choose the device you want to add.
- c) Fill out other meeting information as needed, and send the invitation.
- d) When the meeting is scheduled to begin, verify that the **Join** button appears on the device.

### Step 2

To test a Personal Room meeting in Exchange or Office 365:

- a) In Outlook, Outlook Web Access, or <https://mail.office365.com>, create a new meeting, and then add **@webex** (or the scheduler's Personal Room URL) to the **Location** field.
- b) Go to the Scheduling Assistant and click **Add room**, and choose the device you want to add.
- c) Fill out other meeting information as needed, and send the invitation.
- d) When the meeting is scheduled to begin, verify that the **Join** button appears on the device.

## What to do next

### Introduce the calendar features to your users

Follow these articles to help users learn about the Hybrid Calendar scheduling and out of office features:

- [Schedule a Cisco Webex Meeting from Your Calendar](#)
- [Show When You're Out of Office](#)