Deploy Expressway Calendar Connector for Microsoft Exchange

- Hybrid Calendar Service with Exchange Deployment Task Flow, on page 1
- Configure a Throttling Policy and Apply it to the Impersonation Account, on page 2
- Register Expressway-C Connector Hosts to the Cisco Webex 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 the Hybrid Calendar Service Localizes Meeting Join Details, on page 10
- Start the Calendar Connector, on page 11
- Enable the Hybrid Calendar Service for Users, on page 11
- Register Devices for Calendar Scheduling, on page 12
- Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 13
- Test OBTP with Room or Desk Devices or Webex Boards, on page 14

Hybrid Calendar Service with Exchange Deployment Task Flow

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

Before you begin
Prepare Your Environment

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure a Throttling Policy and Apply it to the Impersonation Account, on page 2</td>
<td>A custom throttling policy helps the Calendar Connector work smoothly.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Register Expressway-C Connector Hosts to the Cisco Webex Cloud</td>
<td>Add the Hybrid Calendar Service to your organization and connect your Expressway to the Cisco Webex cloud. This creates a resource in <a href="https://admin.webex.com">https://admin.webex.com</a> and downloads connector software on to the Expressway.</td>
</tr>
</tbody>
</table>
## Purpose

### Command or Action

**Step 3**  
(Optional) Append the Exchange CA Certificate to the Expressway Trusted CA List, on page 6  
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.

**Step 4**  
Link the Calendar Connector to Microsoft Exchange, on page 7  
Configure Exchange Servers for the Calendar Connector.

**Step 5**  
(Optional) Configure the Calendar Connector's Webex Site Settings, on page 9  
If you have a Cisco Webex Meetings site, configure the @Webex functionality.

**Step 6**  
(Optional) Choose How the Hybrid Calendar Service Localizes Meeting Join Details, on page 10  
To override how the Calendar Connector localizes meeting join details for your entire organization, set the Default Language setting in https://admin.webex.com.

**Step 7**  
Start the Calendar Connector, on page 11

**Step 8**  
Enable the Hybrid Calendar Service for Users, on page 11

**Step 9**  
(Optional) Register Devices for Calendar Scheduling, on page 12  
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 Cisco Webex cloud, configure places for the devices.

**Step 10**  
(Optional) Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 13  
For OBTP on Cisco Webex room and desk devices and Webex Boards, make sure that meeting schedulers have their Webex Personal Rooms associated with their Webex Teams accounts.

**Step 11**  
Test OBTP with Room or Desk Devices or Webex Boards, on page 14  
If you configured OBTP in the previous steps, test it with a device.

## Configure a Throttling Policy and Apply it to the Impersonation Account

A custom throttling policy helps the Calendar Connector work smoothly:

- In Exchange Server 2013 and 2016, the policy removes EWS limits from the impersonation account, to avoid maxconcurrency issues.

- In Exchange Server 2010, the policy overrides the default policy. The default is tailored for user load, not for an enterprise application.
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.
• For Exchange Server 2013 or 2016, enter:
  ```powershell
  New-ThrottlingPolicy -Name "CalendarConnectorPolicy" -EWSMaxConcurrency unlimited
  -EWSMaxBurst unlimited -EWSRechargeRate unlimited -EWSCutOffBalance unlimited
  -EWSMaxSubscriptions 5000
  ```
• For Exchange Server 2010, enter:
  ```powershell
  New-ThrottlingPolicy -Name "CalendarConnectorPolicy" -EWSMaxConcurrency $null
  -EWSPercentTimeInAD 100 -EWSPercentTimeInCAS 500 -EWSPercentTimeInMailboxRPC 300
  -EWSMaxSubscriptions 5000 -EWSFastSearchTimeoutInSeconds 60 -EWSFindCountLimit 1000
  ```

Step 2 If you're using Exchange Server 2013 or 2016, and the impersonation account does not have a mailbox, run
the following command:
```powershell
Enable-Mailbox "impersonation account" -Database "database name"
```

Step 3 Apply the new policy to the impersonation account:
```powershell
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:
```powershell
Get-ThrottlingPolicyAssociation -Identity "impersonation account" | findstr "ThrottlingPolicy"
```

Step 5 On each Exchange 2010 server that has the CAS role, restart the Microsoft Exchange RPC Client Access
service.

What to do next
Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 4
Register Expressway-C Connector Hosts to the Cisco Webex Cloud

Cisco Webex Hybrid Services use software connectors to securely connect Cisco 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 (the software connector host).

Before you begin

- Make sure your Expressway-C is running on a version that's supported for hybrid services. See the Expressway Connector Host Support for Cisco Webex Hybrid Services (https://collaborationhelp.cisco.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

From the customer view in https://admin.webex.com, go to Services, 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 Cisco Webex cloud rejects any attempt at registration from the Expressway web interface. You must first register your Expressway through Cisco Webex 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 2

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 Cisco 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 Cisco Webex 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.
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 3**  
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 4**  
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 Cisco Webex to add those certificates for you.

Choose one of the following options:

- Check the box if you want Cisco 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 Cisco 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 Cisco 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 5**  
Click **Register**. After you’re redirected to Cisco Webex Control Hub, read the on-screen text to confirm that Cisco Webex identified the correct Expressway-C.

**Step 6**  
After you verify the information, click **Allow** to register the Expressway-C for Cisco Webex 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 Cisco Webex 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 Cisco Webex 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the Expressway-C connector host, go to Maintenance &gt; Security certificates &gt; Trusted CA certificate.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Review the CA certificates in the trust list to check if the correct CA certificate is already trusted.</td>
</tr>
</tbody>
</table>
| Step 3 | To append any new CA certificates:  
a) Click Browse (or the equivalent in your browser) to locate and select the PEM file.  
b) 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:  
a) Check the check box next to the Issuer details.  
b) Click Delete.  
c) 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 Cisco Webex Hybrid Services.

If you opted to have Cisco 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 Cisco 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).
<table>
<thead>
<tr>
<th>Cloud hosts signed by this CA</th>
<th>Issuing CA</th>
<th>Must be trusted by</th>
<th>For this purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDN</td>
<td>O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root</td>
<td>Expressway-C</td>
<td>To ensure Expressway downloads connectors from a trusted host</td>
</tr>
<tr>
<td>Common identity service</td>
<td>O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority</td>
<td>Windows Server 2003 or Windows Server 2008 hosting the Cisco Directory Connector Expressway-C</td>
<td>To synchronize users from your Active Directory with Cisco Webex and to authenticate Cisco Webex Hybrid Services users</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority</td>
<td>Expressway-C</td>
<td></td>
</tr>
</tbody>
</table>

**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 Cisco Webex 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.

**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 2010, 2013, or 2016. (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 2010 and later 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.

a) 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 **ldaps** (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 Cisco Webex 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 Cisco 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 **associate their Cisco Webex Personal Room with Cisco Webex Teams in the app.**

**Before you begin**

* For the @webex functionality to work for users, verify the following:

  * You have at least one Cisco 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 Cisco Webex Teams login address. If it does not, users must associate their Cisco Webex Personal Room with Cisco Webex Teams in the 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
On the Expressway-C, go to Applications > Hybrid Services > Calendar Service > Cisco Webex Configuration, and then click New.

Step 2
Enter the Fully Qualified Site Name for this Cisco Webex Meetings site.

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

Step 3
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 4
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 Teams app (either because the user's Webex site has been linked to Webex Teams by an administrator, or because the user configured the setting with a different site).

Step 5
Click Save to save the configuration.

Choose How the Hybrid Calendar Service Localizes Meeting Join Details

In Cisco Webex Control Hub, the Default Language setting controls the language of the join details that the Hybrid Calendar Service 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
From the customer view in https://admin.webex.com, go to Services.

Step 2
From the Hybrid Calendar card for Exchange, click Edit settings.

Step 3
Choose a language from the Default Language drop-down list.
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.

Before you begin

Configure the Calendar Connector's Webex Site Settings, on page 9

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 the Hybrid Calendar Service for Users, on page 11

Enable the Hybrid Calendar Service for Users

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

See Ways to Add and Manage Users in Your Cisco Webex 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 Cisco Webex Teams 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

Cisco Webex users must already be assigned a paid license that provides them with core Cisco Webex messaging and meeting capabilities.
Procedure

**Step 1** From the customer view in [https://admin.webex.com](https://admin.webex.com), go to Users.

**Step 2** 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 3** 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 4** 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.

Users receive an email that indicates the feature is enabled. See the documentation below if you want to disable email notifications.

---

**Register Devices for Calendar Scheduling**

**Before you begin**

**Cisco Webex Calling:**

- After you add a Cisco Webex Calling (formerly Spark Call) phone number to a Cisco Webex room device or board, there is a 24-hour delay before the room device caller ID is seen by others.

- Shared desk phones support all available call features except voicemail and single number reach. Room devices and Webex Boards only support basic call functions with a single line.

- For PSTN service, be aware of the following points:
  - Cloud PSTN service for room devices and boards is available in the United States and Canada.
  - You must request that your Cisco partner purchase PSTN service. If you're no longer in a trial, you must then sign the PSTN contract by DocuSign that is emailed to you.
  - Your partner must add new or port over PSTN numbers.

**Hybrid Call Service:**

- To use Cisco Unified Communications Manager call control for devices in a place, you must first configure Hybrid Call Service Connect for your organization. For more information, see the Deployment Guide for Cisco Webex Hybrid Call Service.

**Procedure**

**Step 1** From the customer view in [https://admin.webex.com](https://admin.webex.com), go to Places, and then click Add Place.

**Step 2** Enter a name for the place (such as the name of the physical room), and then click Next.

**Step 3** Choose Other Cisco device, and then click Next.
You can only have one type of device in a single space. For example, you can add up to 10 desk phones to a lobby or a single Cisco Webex Room Device or a Webex Board, but not a combination of the two.

**Step 4** Choose a call service to assign to devices in the place:

- **Free Calling (default)**—For Cisco Webex Teams app and SIP address calling.
- **Cisco Webex Calling (formerly Spark Call)**—To add PSTN service through a cloud preferred media provider. Assign a phone number and extension to the device, and then click Next.
- **Cisco Webex Hybrid Call Service Connect**—To use call service (PSTN access or internal extension access) through your on-premises call control. Unified CM provides the phone number or extension for the devices in the place.

The service discovers where the email address is located on a Unified CM cluster. Once discovered, the service creates the Cisco Spark-RD and identifies the directory number and SIP URI associated with the account.

**Step 5** (Optional) Toggle on the calendar service so that people can use One Button to Push (OBTP) on this device, and then click Next.

**Step 6** If you chose Hybrid Call Service Connect, enter the Unified CM mail ID for the account that you created earlier, optionally choose the Resource Group that the local Call Connector belongs to, and then click Done.

**Step 7** If you toggled on the calendar service, enter or paste the email address of the calendar mailbox for the room device. This is the email address that is used to schedule meetings.

  - For devices that will be scheduled in Google Calendar, enter the Google resource email address from G Suites (Calendar > Resources). See About calendar resources (rooms, etc) for more information.
  - For devices that will be scheduled in Microsoft Exchange or Office 365, enter the email address of the room mailbox. See Create and Manage Room Mailboxes for more information.

**Step 8** Click Next, and then activate the device with the code provided.

Places that you added Hybrid Call Service to may take approximately 5 to 10 minutes to activate while the email address, directory URI, and directory number are discovered on a Cisco Unified Communications Manager cluster. After activation, the phone number is displayed on Cisco Webex devices in the hybrid-enabled Place.

---

**Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams**

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

- The Webex site is managed on Cisco Webex Control Hub.
- The users on your Webex site have been Cisco Webex Teams linked. (For site linking steps, see Link Webex Sites to Control Hub for Cisco Webex Teams and Analytics.)
- Users associate their Personal Room with Cisco Webex Teams for themselves.
Do this task for the test user account that you'll use to verify the setup, to check whether the Personal Room association needs to be added.

**Procedure**

**Step 1** Sign into the Cisco Webex Teams app.

**Step 2** Go to **Meetings**.

**Step 3** Under **My Personal Room**, if the Personal Room link is missing, enter it in the format `https://company.webex.com/meet/username` or `company.webex.com/meet/username`, enter your host PIN, and select **Save**.

**Step 4** If the link was missing, have users who will schedule meetings that include room or desk devices or boards associate their Personal Rooms with Cisco Webex Teams themselves.

---

**Test OBTP with Room or Desk Devices or Webex Boards**

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](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](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 Service scheduling and out of office features:

- Schedule a Cisco Webex Meeting from Your Calendar.
- Show When You're Out of Office.
Test OBTP with Room or Desk Devices or Webex Boards