Deployment Guide for Cisco Webex Hybrid Calendar Service

First Published: 2017-03-21
Last Modified: 2018-10-18

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

## PREFACE

- New and Changed Information vii

## OVERVIEW OF HYBRID CALENDAR SERVICE

- Hybrid Calendar Service Features xiii
- Simple Meeting Scheduling xiii
- Meetings List and Join Button xiv
- Address Parsing for Video Devices xiv
- Skype for Business Addresses (Available for Exchange and Office 365 Integrations) xv
- Out-of-Office Status (Available for Exchange and Office 365 Integrations) xv
- Expressway-Based Calendar Connector for Microsoft Exchange and Office 365: Architecture xvi
- Office 365 and Hybrid Exchange Environments xviii
- Cloud-Based Hybrid Calendar Service with Office 365: Scheduling Flow xix
- Hybrid Calendar Service with Google Calendar: Scheduling Flow xx

## PART I

**Microsoft Exchange or Office 365 with Expressway Calendar Connector** 23

## CHAPTER 1

**Prepare Your Environment** 1

- Management Connector 1
- Calendar Connector 1
- Choosing Between the Calendar Connector and the Cloud-based Service for Office 365 Users 2
- Requirements for Hybrid Calendar Service 3
- Set Up an Impersonation Account for On-Premises Microsoft Exchange 3
- Set Up an Impersonation Account for Office 365 4
- Complete the Prerequisites for Hybrid Calendar Service 5
- Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services 6
Deploy Expressway Calendar Connector for Microsoft Exchange

Hybrid Calendar Service with Exchange Deployment Task Flow

Configure a Throttling Policy and Apply it to the Impersonation Account

Register Expressway-C Connector Hosts to the Cisco Webex Cloud

Append the Exchange CA Certificate to the Expressway Trusted CA List

Certificate Authorities for Hybrid Services

Link the Calendar Connector to Microsoft Exchange

Configure the Calendar Connector's Webex Site Settings

Start the Calendar Connector

Enable the Hybrid Calendar Service for Users

Register Devices for Calendar Scheduling

Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams

Test OBTP with Room or Desk Devices or Webex Boards

Deploy Expressway Calendar Connector with Office 365

Hybrid Calendar Service with Office 365 Deployment Task Flow

Register Expressway-C Connector Hosts to the Cisco Webex Cloud

Append the Exchange CA Certificate to the Expressway Trusted CA List

Certificate Authorities for Cisco Webex Hybrid Services in an Office 365 Environment

Link Calendar Connector to Office 365

Configure the Calendar Connector's Webex Site Settings

Start the Calendar Connector

Enable the Hybrid Calendar Service for Users

Hybrid Exchange and Office 365 Deployments

Deploy Hybrid Calendar Service for a Hybrid Exchange Environment

Deploy Expressway Calendar Connector for a Hybrid Exchange Environment

Office 365 with Cloud-Based Hybrid Calendar Service

Prepare Your Environment

How the Hybrid Calendar Service Accesses User Calendars
Deploying Alongside an Existing Expressway-Based Calendar Connector 42
Change Processing Timeframes 42
Requirements for Hybrid Calendar Service with Microsoft Office 365 43

CHAPTER 6

Deploy Cloud-Based Hybrid Calendar Service for Office 365 45
Hybrid Calendar Service with Office 365 Deployment Task Flow 45
Prepare Your Cisco Webex Meetings Site 46
Enable and Configure Hybrid Calendar Service with Office 365 46
Enable the Hybrid Calendar Service with Office 365 for Users 47
Register Devices for Calendar Scheduling 48
Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams 49
Test the Office 365 and Hybrid Calendar Service Integration 50
Move a User from an Expressway-Based Connector 50

PART IV

Google Calendar 53

CHAPTER 7

Prepare Your Environment 55
Requirements for Hybrid Calendar Service With Google Calendar 55
Remove Google Hangouts Information in Meeting Events 55

CHAPTER 8

Deploy Hybrid Calendar with Google Calendar 57
Enable and Configure Hybrid Calendar Service with Google Calendar 57
Enable the Hybrid Calendar Service with Google for Users 58
Register Devices for Calendar Scheduling 59
Have Users Associate Their Personal Rooms with Cisco Webex Teams 60
Test the Google Calendar And Hybrid Calendar Service Integration 61

APPENDIX A

Known Issues with Hybrid Calendar Service 63
Exchange and Office 365 (Expressway-Based Calendar Connector) 63
Office 365 (Cloud-Based Service) 65
Google Calendar (Cloud-Based Service) 67

APPENDIX B

Troubleshoot Hybrid Calendar Service 69
Diagnostic Tools on Expressway-C Connector Host 69
Check Connector Health on Expressway-C  69
Roll Back to the Previous Version of a Connector  70

APPENDIX C

Important Items for Hybrid Services Deployments  73
Supported Certificate Authorities  73
Exchange Impersonation Account  75
New and Changed Information

This table covers new features or functionality, changes to existing content, and any major errors that were fixed in the Deployment Guide.

For information about Calendar Connector software updates, see the Calendar Connector Release Notes.

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
</table>
| October 18, 2018    | • Updated the requirements for each of the calendar integrations to note the following:  
                        Each Webex Teams user can only have one email address associated with only one Hybrid Calendar Service integration. In other words, the Hybrid Calendar Service will only process meetings from a single address for creating spaces, decorating meetings, showing the meetings list and join button, and sending One Button to Push (OTBP) to video devices. |
| October 17, 2018    | • Updated the permissions in How the Hybrid Calendar Service Accesses User Calendars, on page 41 (for the new Office 365 cloud-based service) to include writing user mailbox settings.  
                        • Updated Known Issues for Office 365 (Cloud-Based Service), on page 65. |
| October 11, 2018    | • Added mention of new cloud-based service in Deploy Expressway Calendar Connector for a Hybrid Exchange Environment, on page 37.  
                        • Updated Known Issues for Exchange and Office 365 (Expressway-Based Calendar Connector), on page 63. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 24, 2018</td>
<td>• For the Expressway-based Calendar Connector, added deployment steps to access the new Autodiscover Redirect URL trust list (Applications &gt; Hybrid Services &gt; Calendar Service &gt; Autodiscover Redirect URL Configuration). Running an Autodiscover test automatically adds URLs to the list in pending state, or administrators can add URLs to the list manually. Pending URLs are blocked unless an administrator chooses to allow them.</td>
</tr>
</tbody>
</table>
| August 30, 2018   | • Added content for the new cloud-based Hybrid Calendar Service with Office 365:  
  • For a feature overview, see Overview of Hybrid Calendar Service, on page xiii.  
  • For deployment instructions, see the "Office 365 with Cloud-Based Calendar Service for Office 365" part of this guide, which includes the following chapters:  
    • Prepare Your Environment, on page 41  
    • Deploy Cloud-Based Hybrid Calendar Service for Office 365, on page 45  
  • For known issues, see Known Issues with Hybrid Calendar Service, on page 63  
  • For the Expressway-based Hybrid Calendar Service with Microsoft Exchange or Office 365, made the following changes in Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 6:  
    • Added a note advising not to change the MAC address of the Expressway virtual machine because the serial number is based on the MAC address.  
    • Added a note explaining how to enable H.323 mode if you do not have the UI menu on Expressway.  
  • Removed most references to @spark, which will be deprecated. Currently, users can enter "@webex:space" or "@meet" instead of "@spark". |
| July 25, 2018     | • Added Webex Board as an additional device that supports One Button to Push.  
  • Updated the Known Issues list. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
</table>
| May 30, 2018 | • Changed terminology to reflect the rebranding of Cisco Spark:  
|              |   • Cisco Spark Hybrid Calendar Service is now Cisco Webex Hybrid Calendar Service.  
|              |   • The Cisco Spark app is now the Cisco Webex Teams app.  
|              |   • The Cisco Collaboration Cloud is now the Cisco Webex cloud.  
|              |   Other product names, documents, and images may not immediately reflect these changes.  
|              |   • Updated the Overview of Hybrid Calendar Service, on page xiii to clarify that the Skype for Business address feature is currently only available for Microsoft Exchange and Office 365 integrations, not for Google integrations. |
| May 14, 2018 | • Split the Overview of Hybrid Calendar Service, on page xiii into feature sections, and added links to related articles for users. Added new sections for address parsing and Skype for Business addresses.  
|              |   • For Exchange and Office 365 deployments, clarified when the Webex site that is configured as the "default" is used, in the Configure the Calendar Connector's Webex Site Settings, on page 19.  
|              |   • Updated the topics on enabling the Hybrid Calendar Service for users to indicate that you can add and verify your domain if you want users to be able to use @webex without having to sign in to the Cisco Spark app.  
|              |   • Updated the Known Issues list.                                                                                                                                                                           |
| April 10, 2018 | • For hybrid calendar environments with both on-premises Exchange and Office 365, added information on how to use a single impersonation account and Expressway-C Exchange configuration record to set up the integration. |
| March 21, 2018 | • Removed references to @webex:sitename.  
<p>|              |   • Added task to Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 23 to the Hybrid Calendar Service with Exchange and the Hybrid Calendar Service with Office 365 deployment task flows. This task is required to provide OBTP to Cisco Spark room and desk devices when scheduling Webex Personal Room meetings. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
</table>
| March 8, 2018      | • Removed references to Webex versions WBS29 and WBS30, as these versions have reached end-of-support.  
                          • Updated @webex requirements: the Personal Room feature must be enabled for the Webex site and for the individual users.  
                          • For One Button to Push (OBTP) on Cisco Spark room and desk devices with Google Calendar, clarified the requirement that users have their Webex Personal Room link associated with their Cisco Spark account. (This can happen in multiple ways.)  
                          • Moved Expressway-C cluster user capacity numbers out of Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 6 and into User Capacity Limits for Expressway-based Cisco Spark Hybrid Services.                                                                 |
| February 19, 2018  | • Added meetings list and **Join** button (also known as One Button to Push, or OBTP) for the Cisco Spark app for Mac and Windows to the features list for Google calendar deployments.  
                          • Added **Join** button (OBTP) for the Cisco Spark room and desk devices to the features list for Google calendar deployments.  
                          • Added steps to deploy OBTP on Cisco Spark room and desk devices for Google Calendar integrations.  
                          • Updated email address requirement in Configure the Calendar Connector's Webex Site Settings, on page 19.                                                                                                                                                                              |
| February 1, 2018   | • Updated the requirement for user email addresses to match between the calendar system, Cisco Spark, and Webex in Requirements for Hybrid Calendar Service, on page 3 and Requirements for Hybrid Calendar Service With Google Calendar, on page 55.  
                          • Updated hyperlinks to related articles on alternative ways to enable the Hybrid Calendar Service for users.                                                                                                                                                                                                                              |
| January 12, 2018   | • Updated Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 6 with capacity numbers for a Hybrid Exchange (on-premises and Office 365) environment.  
                          • Changed the link for Expressway software from admin.ciscospark.com to software.cisco.com.  
                          • In Exchange, Office 365, and Hybrid Exchange sections, added the recommendation to check both NTLM and Basic authentication for Hybrid Exchange deployments.                                                                                                                                                    |
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 20, 2017</td>
<td>• Updated the Known Issues list.</td>
</tr>
<tr>
<td></td>
<td>• Removed a duplicate copy of the &quot;Certificate Authorities for Cisco Spark Hybrid Services&quot; section.</td>
</tr>
<tr>
<td>November 17, 2017</td>
<td>• For Microsoft Exchange and Office 365, specified that you should not use the same impersonation account as other services such as Cisco Unity Connection, Cisco TMSXE, and so on.</td>
</tr>
<tr>
<td></td>
<td>• Added *.clouddrive.com to the list of sites that the Expressway-C must be able to reach (for Microsoft Exchange and Office 365).</td>
</tr>
<tr>
<td></td>
<td>• Updated the Known Issues list.</td>
</tr>
<tr>
<td></td>
<td>• Updated the description of the &quot;One Button to Push Topology: Cloud-Registered Cisco Spark Room and Desk Devices&quot; figure.</td>
</tr>
<tr>
<td>November 9, 2017</td>
<td>• Added *.rackcdn.com to the list of sites that the Expressway-C must be able to reach (for Microsoft Exchange and Office 365).</td>
</tr>
<tr>
<td></td>
<td>• Updated the Known Issues list.</td>
</tr>
<tr>
<td>October 13, 2017</td>
<td>Updated the Overview section and the Microsoft Exchange and Office 365 section of the guide with information on the new Cisco Spark app meeting list feature and additional One Button to Push (OBTP) support.</td>
</tr>
</tbody>
</table>
Overview of Hybrid Calendar Service

• Hybrid Calendar Service Features, on page xiii
• Expressway-Based Calendar Connector for Microsoft Exchange and Office 365: Architecture, on page xvi
• Office 365 and Hybrid Exchange Environments, on page xviii
• Cloud-Based Hybrid Calendar Service with Office 365: Scheduling Flow, on page xix
• Hybrid Calendar Service with Google Calendar: Scheduling Flow , on page xx

Hybrid Calendar Service Features

With Hybrid Calendar Service, you can connect your on-premises Microsoft Exchange, Office 365 or Google's G Suite Calendar (Google Calendar) environment to Cisco Webex. This integration makes it easier to schedule and join meetings, especially when mobile; no plugins are required.

Hybrid Calendar Service has no Cisco call control dependency—you can use this service to extend features to Cisco Webex users, even if you use a third-party UC solution.

Simple Meeting Scheduling

To simplify scheduling a meeting, your users can type scheduling keywords and modifiers in the location field of their calendar invitation:

<table>
<thead>
<tr>
<th>To Do This…</th>
<th>Use Any of These in the Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Cisco Webex Teams space for meetings, or host the meeting through Cisco Webex Teams.</td>
<td>• @webex:space</td>
</tr>
<tr>
<td></td>
<td>• @meet</td>
</tr>
<tr>
<td></td>
<td>• @meet:space</td>
</tr>
<tr>
<td></td>
<td>• @spark (deprecated)</td>
</tr>
</tbody>
</table>
### Meetings List and Join Button

The meetings list in Cisco Webex Teams lets users see upcoming meetings for the next 4 weeks. Users see a **Join** button in the meetings list and a scheduled meeting notification 5 minutes before the meeting starts.

Users can add Cisco Webex room and desk devices and Webex Boards to a meeting to make conferencing resources available. If the device is enabled for the Hybrid Calendar Service, the green **Join** button appears on the device. (The **Join** button is also known as One Button to Push, and is also available to devices that are registered to Cisco Unified Communications Manager, and managed by Cisco TelePresence Management Suite.) Hybrid Calendar Service-enabled room and desk devices can also show meetings to which they've been invited in the meetings list.

**Related Topics**
- View Upcoming Meetings in Cisco Webex Teams
- Join a Scheduled Meeting in Cisco Webex Teams

### Address Parsing for Video Devices

In addition to the scheduling keywords, the Hybrid Calendar Service can parse a SIP URI or other video address from the body of a calendar invitation, even if it's not a Webex standard meeting, Webex Personal Room meeting, or Webex team meeting address. When the address matches a supported format, the meeting appears in invitees' meetings lists and meeting notifications in the Webex Teams app. The meeting also appears in the list on any scheduled room or desk devices that are enabled for the Hybrid Calendar Service, and the devices show the green Join button (One Button To Push) just before the meeting starts.

The meeting organizer must be enabled for the Hybrid Calendar Service, and the address must match a supported format.

**Table 1: Supported Video Address Format Examples**

<table>
<thead>
<tr>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard SIP address</td>
<td>sip:<a href="mailto:jdoe@company.com">jdoe@company.com</a></td>
</tr>
<tr>
<td></td>
<td>sips:<a href="mailto:jdoe@company.com">jdoe@company.com</a></td>
</tr>
<tr>
<td>Special-case URI—all numbers without sip: prefix</td>
<td><a href="mailto:12345@company.com">12345@company.com</a></td>
</tr>
</tbody>
</table>
Table 2: Unsupported Video Address Format Examples

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SIP protocol address</td>
<td><a href="mailto:12345@example.com">mailto:12345@example.com</a></td>
</tr>
<tr>
<td>Incomplete SIP address</td>
<td>sip:12345</td>
</tr>
</tbody>
</table>

Related Topics

Meetings with Video Addresses in Your Cisco Webex Teams Meeting List

Skype for Business Addresses (Available for Exchange and Office 365 Integrations)

When adding Cisco Webex Meetings join details to an invitation, the Hybrid Calendar Service now also includes a Skype for Business-specific video address.

Related Topics

Start or Join a Webex Video Meeting Using Skype for Business

Out-of-Office Status (Available for Exchange and Office 365 Integrations)

From Outlook, your users can share their out-of-office status to other users in Cisco Webex Teams. As soon as a user sets an automatic reply and date range, other users can see the status in Webex Teams in these locations:

- In @mentions directed at the out-of-office user.
- In the People space for that user.
- In search results for that user's name.
- In the expanded people roster for a space.

Note

This feature is currently only available with Exchange and Office 365 integrations that use the Expressway-based Calendar Connector. If you use the Calendar Connector and add the new cloud-based Hybrid Calendar Service for Microsoft Office 365, any Office 365 users who are not in a resource group will automatically migrate from the Connector to the cloud-based service. Make sure that these users know they will lose this functionality until it is implemented in the cloud-based service. If out-of-office status is important to your users, consider waiting to deploy the new cloud-based service until the feature is available.

Related Topics

Show When You're Out of Office
Expressway-Based Calendar Connector for Microsoft Exchange and Office 365: Architecture

For a detailed overview of Cisco Webex Hybrid Services, including architectural and design information for the Expressway-based Calendar Connector, we recommend that you read the Preferred Architecture for Cisco Webex Hybrid Services, Design Overview.

For more information on how the Calendar Connector integrates with Microsoft Exchange and Office 365, see the Cisco Webex Hybrid Calendar Service with Microsoft Exchange Integration Reference.

**Figure 1: Exchange (on-premises and cloud), Connector, and Cisco Webex Cloud Components for Hybrid Calendar Service**

This diagram shows the components of Hybrid Calendar Service architecture and where the Expressway-based Connectors integrate the on-premises components with the cloud.

**Figure 2: One Button to Push Topology: Cloud-Registered Cisco Webex Room and Desk Devices**

This diagram shows the One Button to Push (OBTP) topology for cloud-registered room and desk devices and Webex Boards. The cloud activates OBTP for meetings with a scheduling keyword or supported video
address when these devices are included as invitees.

*Figure 3: One Button to Push Topology: Cisco Unified Communications Manager and Cisco TMS*

This diagram shows Hybrid Calendar Service and Cisco TMS providing one button to push (OBTP) to Cisco Unified Communications Manager-registered video endpoints for meetings with a scheduling keyword or supported video address when these devices are included as invitees.
Office 365 and Hybrid Exchange Environments

Previously, to serve Office 365 users, you had to install the Calendar Connector on an on-premises Expressway. This on-premises deployment was required even if you didn't have a hybrid Exchange environment (on-premises Microsoft Exchange and an Office 365 tenant organization).

You can now choose to enable the cloud-based Hybrid Calendar Service for Office 365. With this service, hybrid Exchange environments have extra considerations:

- You can run the Expressway-based Calendar Connector and the cloud-based Office 365 service at the same time.
- Once you enable the cloud-based service, all Office 365 users who are not in any resource group automatically migrate to it.
- To test the migration on a subset of users, make sure that the rest of the Office 365 users are in a resource group. Then enable the cloud-based Office 365 service.

Figure 4: Hybrid Exchange Environment with the Cisco Webex Hybrid Calendar Service

The Calendar Connector on the Expressway-C serves both Exchange users and Office 365 users, in Resource Group A and Resource Group B. The cloud-based service serves any Office 365 users who are not in a resource group.
Cloud-Based Hybrid Calendar Service with Office 365: Scheduling Flow

1. A user creates a meeting in the Office 365 calendar, putting a scheduling keyword or video address in the Location field.
2. Exchange Online sends a notification to the Hybrid Calendar Service.
3. The Hybrid Calendar Service requests and receives the encryption key, and then uses it to encrypt the meeting information.
4. The Hybrid Calendar Service validates meeting creation and recipients, and then creates a Webex team space, if applicable.
5. The Hybrid Calendar Service calls the API service and, if applicable, maps the meeting to the space.
6. The Hybrid Calendar Service retrieves the meeting join information, including the Webex Personal Room if applicable.
7. The Hybrid Calendar Service updates the meeting invite with the meeting join information and, if applicable, the space ID.
8. The invitees and the organizer get the updated meeting invitation.
For more information on how the cloud-based Hybrid Calendar Service integrates with Office 365, see the Cisco Webex Hybrid Calendar Service with Office 365 Integration Reference.

Hybrid Calendar Service with Google Calendar: Scheduling Flow

This diagram shows the components of Hybrid Calendar Service and Google Calendar architecture.

1. A user creates a meeting in Google Calendar, putting a scheduling keyword or video address in the location field.
2. Google sends a notification to the Hybrid Calendar Service.
3. The Hybrid Calendar Service requests and receives the encryption key, and then uses it to encrypt the meeting information.
4. The Hybrid Calendar Service validates meeting creation and recipients, and then creates a Webex team space, if applicable.
5. The Hybrid Calendar Service calls the API service and maps the meeting to the space.
6. The Hybrid Calendar Service retrieves the meeting join information, including the Personal Room if applicable.
7. The Hybrid Calendar Service updates the meeting invite with the meeting join information and, if applicable, the space ID.

8. The updated meeting information appears in Google Calendar.

For more information on how the Hybrid Calendar Service integrates with Google's G Suite Calendar, see the Cisco Webex Hybrid Calendar Service with Google Calendar Integration Reference.
PART I

Microsoft Exchange or Office 365 with Expressway Calendar Connector

• Prepare Your Environment, on page 1
• Deploy Expressway Calendar Connector for Microsoft Exchange, on page 11
• Deploy Expressway Calendar Connector with Office 365, on page 25
CHAPTER 1

Prepare Your Environment

- Management Connector, on page 1
- Calendar Connector, on page 1
- Choosing Between the Calendar Connector and the Cloud-based Service for Office 365 Users, on page 2
- Requirements for Hybrid Calendar Service, on page 3
- Set Up an Impersonation Account for On-Premises Microsoft Exchange, on page 4
- Set Up an Impersonation Account for Office 365, on page 5
- Complete the Prerequisites for Hybrid Calendar Service, on page 6
- Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 7

Management Connector

The Management Connector is included in the Expressway-C base. You use it to register an Expressway to the cloud and link the Expressway interface with Cisco Webex Control Hub. The Management Connector plays an important role as the coordinator of all connectors running on the Expressway server or cluster: It provides you with a single point of control for connector activities. The Management Connector enables cloud-based management of the on-premises connectors, handles initial registration with the cloud, manages the connector software lifecycle, and provides status and alarms.

For an HTTPS connection to be established between the Management Connector and the cloud, you must update the trust list on the Expressway-C connector host with certificates that were signed by certificate authorities in use by the Cisco Webex cloud. You can allow the Cisco Webex cloud to upload CA certificates to the Expressway-C trust store. Or, in the case where security policies prevent the Cisco Webex cloud from uploading trusted certificate authority certificates on Expressway-C, you may upload them manually.

Calendar Connector

The Calendar Connector is the on-premises component of the Hybrid Calendar Service. The connector runs on an Expressway-C host that you register to the Cisco Webex cloud.

The Calendar Connector acts like a broker between the cloud and your Microsoft Exchange (on-premises), Office 365 (cloud), or both (Hybrid Exchange deployment). The connector acts on behalf of users, similar to the way a client application would access a user’s calendar information. The connector uses the impersonation role (which you can restrict to a subset of users) and uses Exchange Web Services to:
• Autodiscover where users are homed
• Listen for notifications on a user's calendar
• Retrieve information on a user's calendar items and Out-of-Office status
• Populate meeting invitations with details of Cisco Webex Teams spaces and Webex personal rooms.

The Hybrid Calendar Service is designed to minimize security concerns in a hybrid environment:
• The cloud cannot retrieve or access the Exchange credentials from the connector
• The cloud has no direct access to Exchange through the connector
• The connector does not access any user email or contacts
• The connector does not create search folders or other extra folders for the user
• The connector is not an Exchange Foreign connector
• The connector does not interact with the Exchange Hub transport server
• No AD schema extensions are required

In production Exchange, the Calendar Connector increases the CPU usage and load on the CAS and MBX servers. The impact on your Exchange environment depends on:
• Your Exchange deployment
• The number of configured users
• The number of meetings that the Hybrid Calendar Service updates per user per hour
• The size of calendars

We document a throttling policy designed to help manage the increased traffic.

**Choosing Between the Calendar Connector and the Cloud-based Service for Office 365 Users**

With the release of the cloud-based service for Office 365 users, you can now choose whether to deploy only the Expressway-based Calendar Connector, a combination of the Calendar Connector and the cloud-based service, or, if you have no Microsoft Exchange users, deploy only the cloud-based service.

The cloud-based service can scale beyond the 1000 user limit for Office 365 users and is simpler to deploy and maintain. It does not service Microsoft Exchange users, and currently does not support the out-of-office feature. If you deploy it alongside the Calendar Connector, your Office 365 users automatically move to the cloud-based service (unless they are in resource groups).

Before you decide which service to deploy for your Office 365 users, read the Prepare Your Environment, on page 41 chapter of the Office 365 with Cloud-Based Hybrid Calendar Service part of this guide, to understand the requirements for that option.
Requirements for Hybrid Calendar Service

<table>
<thead>
<tr>
<th>Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Webex Teams</td>
<td>Cisco Webex Hybrid Calendar Service is available with the offers documented in License Requirements for Cisco Webex Hybrid Services.</td>
</tr>
<tr>
<td>Cisco Expressway—download from software.cisco.com at no charge</td>
<td>We recommend the latest release of Expressway for connector host purposes. See Expressway Connector Host Support for Cisco Webex Hybrid Services for information about Expressway version support.</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>• 2010 SP3, 2013, 2016</td>
</tr>
<tr>
<td></td>
<td>• Office 365</td>
</tr>
<tr>
<td>Cisco Webex Meetings—Use for @webex scheduling only; not required for scheduling meetings in Webex team spaces.</td>
<td>Any supported Cisco Webex Meetings release You must enable the Personal Room feature for the Webex site and for the individual users.</td>
</tr>
</tbody>
</table>

Each user's email address in the calendar system (Microsoft Exchange or Office 365) must match their Cisco Webex Teams login address. To use @webex, the address should also match the user's Cisco Webex account address. If it does not, users must associate their Webex Personal Room with Cisco Webex Teams in the app in order to use @webex.

Each Webex Teams user can only have one email address associated with only one Hybrid Calendar Service integration. In other words, the Hybrid Calendar Service will only process meetings from a single address for creating spaces, decorating meetings, showing the meetings list and join button, and sending One Button to Push (OTBP) to video devices.

Set Up an Impersonation Account for On-Premises Microsoft Exchange

Before you begin

- You must choose a mail-enabled account to use as the service account. (The account doesn't have to be an administrator, but it must have a mailbox.)

- Do not use an impersonation account that is used by other services such as Cisco Unity Connection, Cisco TMSXE and so on.

- If you limited the set of users that are synchronized with Active Directory using LDAP filters, you may want to limit the impersonation by using a new or existing management scope in Exchange.

- For instructions and more detailed information from Microsoft on management scopes and impersonation, see:
  - Exchange Server 2013 and 2016
  - Exchange Server 2010
Set Up an Impersonation Account for Office 365

Give impersonation permissions to the service account that the Calendar Connector will use with Office 365.

Before you begin

- For a hybrid Exchange on-premises and Office 365 integration, you can use a simplified configuration with a single impersonation account if your deployment meets all of the following criteria:
  - You synchronize your on-premises Exchange accounts to the Office 365 cloud.
    The impersonation account that you use must also be synchronized the Office 365 cloud, and the account's userPrincipalName must match one of its SMTP addresses.
  - You administer all users in the on-premises Active Directory, including users whose mailboxes have been migrated to the Office 365 cloud.
  - You synchronize passwords, or have a configured a federation so that users have a single password both on-premises and in the cloud.
  - Your Exchange is configured such that all autodiscovery requests reach the on-premises environment.
    (If a mailbox has been migrated, the response indicates the relocation and provides the cloud email address.)

In the simplified configuration, you use a single impersonation account to service all users. Because ApplicationImpersonation privileges that you assign on-premises do not automatically apply to mailboxes homed in the Office 365 cloud, you must still explicitly assign these privileges. To do so, follow this procedure and use the same service account that you used in Set Up an Impersonation Account for
On-Premises Microsoft Exchange, on page 3. Later, you'll set up only one Microsoft Exchange configuration on the Expressway-C.

For a hybrid integration that does not meet these criteria, follow this procedure and use a different service account for impersonation than you used in Set Up an Impersonation Account for On-Premises Microsoft Exchange, on page 3. Later, you'll set up two Exchange configuration records on the Expressway-C: one for the Exchange on-premises integration, and one for the Office 365 integration.

- You must choose a mail-enabled account for this task. (The account doesn't have to be an administrator, but it must have a mailbox.)

- Do not use an impersonation account that is used by other services such as Cisco Unity Connection, Cisco TMSXE and so on.

- Ensure that the service account can authenticate with the authentication service or directory that is used in your deployment.

Procedure

Step 1 Log in to the Office 365 Admin Center using the administrator account.
Step 2 Under Admin, select Exchange.
Step 3 Select Permissions.
Step 4 Under Admin Roles, create a new role group and enter a descriptive name, such as ImpersonationGroup.
Step 5 Under Roles, add a new role. Select ApplicationImpersonation role.
Step 6 Add the role to the group, and then select OK.
Step 7 Add the service account to be used for impersonation to the group.

Related Topics
Exchange Impersonation Account, on page 75

Complete the Prerequisites for Hybrid Calendar Service

Procedure

Step 1 Allow time to configure the impersonation account. See Exchange Impersonation Account to understand the role of the account and for answers to common questions that are related to security.
Step 2 Install or make sure you're running a supported calendar environment, as described in Requirements for Hybrid Calendar Service, on page 3.
Step 3 Ensure that users are listed in Active Directory and have a discoverable mailbox in the organization's Exchange server.
Step 4 (Optional) Download the latest Directory Connector software from Cisco Webex Control Hub (https://admin.webex.com) and use it to import user attributes from your Active Directory. For more information about how to use Directory Connector, see the Deployment Guide for Cisco Directory Connector.
Step 5 Provide the following port access:
• Port access for HTTPS or secure web sockets outbound from Expressway to *.rackcdn.com, *.ciscospark.com, *.wbx2.com, *.webex.com, and *.clouddrive.com: TCP port 443 (secure)
• Port access for EWS outbound from Expressway to Exchange: TCP port 443 (secure) or TCP port 80 (nonsecure)
• Port access for LDAP outbound from Expressway to Active Directory: TCP port 636 (secure) or TCP port 389 (nonsecure)
• Port access for Microsoft Global Catalog search: TCP port 3269 (for Global Catalog search secured by SSL) or TCP port 3268 (for unsecured Global Catalog search).

Step 6  For @webex functionality, configure or use a Cisco Webex Meetings site. You must enable the Personal Room feature for the site and for the individual users.

Step 7  To make One Button to Push (OBTP) available for Unified CM-registered endpoints managed by TMS:
• Set up Cisco TMS 15.0 and Cisco TMSXE 5.0 or higher with Microsoft Exchange integration. See the Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (TMS 15.0 - WebEx Meeting Center WBS30). TMS and XE require no additional configuration to support Hybrid Calendar Service.
• To make conference rooms schedulable in Microsoft Outlook/Exchange, configure them in XE as if you were using on-premises conferencing. To configure rooms in Exchange, use the Cisco TelePresence Management Suite Extension for Microsoft Exchange Administration Guide.

• Understand the licensing requirements:
  • TMS and XE Licensing is the same as if using on-premises resources. You require enough licenses to cover the number of endpoints that will use OBTP. A TMS license is needed to manage the endpoint and to push the speed dial button on the touchpad at the time of the scheduled conference. A TMS-XE license is needed for the endpoint to be scheduled in Exchange.

• For Unified CM-registered endpoints, OBTP works with Hybrid Calendar Service and Productivity Tools plugin for meeting invitations:
  • Hybrid Calendar Service (scheduling keywords or supported video address) populates the user attribute "TMS:ExternalConferenceData" with the SIP URI for TMS to set the OBTP dial string.
  • Productivity Tools plugin populates the attribute "UCCapabilities" attribute with the SIP URI for TMS to set the OBTP dial string.

If you have on-premises conferencing, you can add OBTP with Cisco Webex Meetings and run both at same time. We support OBTP functionality only; auto connect is not available.

Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services

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

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

See User Capacity Limits for Expressway-based Hybrid Services so that you can plan your deployment accordingly.

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 Cisco Webex Control Hub (https://admin.webex.com).

Step 2
Plan your connector capacity by referring to User Capacity Limits for Expressway-based Hybrid Services.

Step 3
Deploy the Expressway-C connector host in a cluster to account for redundancy. Follow the supported Expressway scalability recommendations:

- For Hybrid Calendar Service (Exchange or Office 365) on a dedicated Expressway-C:
  - Calendar Connector supports a single cluster with up to 2 Expressway-C nodes.
  - Calendar Connector can under-provision users. If a single node fails, the system has extra capacity for all users to fail over to the working node. If one of the nodes fails in the cluster, the discovery and assignment services move users to the working node in approximately 30 seconds.
  - The service catches up on any missed notifications if there is an outage.

Cisco Webex Hybrid Services are highly available if Microsoft Exchange, Unified CM, and Cisco Expressways are deployed in a cluster. The same guidelines that apply to Cisco VCS and Expressway apply for the Expressway-C connector host clustering.

Step 4
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 Cisco 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 Cisco Webex 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: Internet Explorer 8 or 9 (not in compatibility mode), Firefox 3 or later, or Chrome.

The interface may work in other browsers, but they are not officially supported. You must enable JavaScript and cookies to use the Expressway web interface.

Step 5

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

Select all the services that apply. For example, you may want this Expressway-C to do both Cisco Webex Hybrid Services and Business to business calls. Select Proceed without selecting services if you prefer to configure the Expressway-C without the wizard.

Step 6

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)

Step 7

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:
  

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 8** If you have not already done so, open required ports on your firewall.

• All traffic between Expressway-C and the Cisco 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](https://collaborationhelp.cisco.com/article/WBX000028782) for details of the cloud domains that are requested by the Expressway-C.

**Step 9** 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**.

**Step 10** Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

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

  You can let Cisco 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.

• Access to the Expressway CA trust list may also be required if you want to secure the connections between Expressway-C and Microsoft Exchange, or between Expressway-C and Microsoft® Active Directory®, when configuring the Calendar Connector.
Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services
Deploy Expressway Calendar Connector for Microsoft Exchange

- Hybrid Calendar Service with Exchange Deployment Task Flow, on page 11
- Configure a Throttling Policy and Apply it to the Impersonation Account, on page 12
- Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 13
- Append the Exchange CA Certificate to the Expressway Trusted CA List, on page 15
- Link the Calendar Connector to Microsoft Exchange, on page 17
- Configure the Calendar Connector’s Webex Site Settings, on page 19
- Start the Calendar Connector, on page 20
- Enable the Hybrid Calendar Service for Users, on page 21
- Register Devices for Calendar Scheduling, on page 22
- Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 23
- Test OBTP with Room or Desk Devices or Webex Boards, on page 24

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, on page 1

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure a Throttling Policy and Apply it to the Impersonation Account, on page 12</td>
<td>A custom throttling policy helps the Calendar Connector work smoothly.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 26</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>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) Append the Exchange CA Certificate to the Expressway Trusted CA List, on page 15</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Link the Calendar Connector to Microsoft Exchange, on page 17</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) Configure the Calendar Connector's Webex Site Settings, on page 19</td>
<td>If you have a Cisco Webex Meetings site, configure the @Webex functionality.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Start the Calendar Connector, on page 20</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enable the Hybrid Calendar Service for Users, on page 21</td>
</tr>
<tr>
<td><strong>Step 8</strong> (Optional) Register Devices for Calendar Scheduling, on page 22</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 9</strong> (Optional) Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 23</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Test OBTP with Room or Desk Devices or Webex Boards, on page 24</td>
</tr>
</tbody>
</table>

## 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, on page 3

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:

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

- For Exchange Server 2010, enter:

  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:

  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"

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 13

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.

  **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 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 16.

---

**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**

**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:

   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>
</tbody>
</table>
Link the Calendar Connector to Microsoft Exchange

The Calendar Connector installs automatically after you register your Expressway 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-C 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 For **Autodiscovery**, select **Use Active Directory** 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 For autodiscovery, configure the extra fields with the AD details.

The Calendar Connector uses the **Active Directory domain**, **Active Directory site**, and **Query mode** fields only for the first step of autodiscovery. In this step, it performs an Active Directory Service Connection Point (SCP) record lookup to get a list of autodiscover URLs. 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.

a) Enter the **Active Directory domain** to query.

b) (Optional) Enter the **Active Directory site** that is geographically closest to the Calendar Connector, to optimize the query response time.

c) 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.

d) 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.
e) Enter an **Email Address** so that Calendar Connector can test the connection and check that the directory query worked.

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 mailbox name, then your settings are saved without verifying connectivity.

**Step 11**

(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 12**

Click **Add** to store the Exchange Server configuration on the Expressway-C.

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

**What to do next**

*Configure the Calendar Connector's Webex Site Settings, on page 19*

---

**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.

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 19

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 21
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 into 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, 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.

What to do next

Test the calendar features

Follow these articles to test the Hybrid Calendar Service scheduling and out of office features with your users:

- Schedule a Cisco Webex Meeting from Your Calendar.
- Show When You're Out of Office.
Register Devices for Calendar Scheduling

Before you begin

Cisco Webex Calling:
- After you add a Cisco Webex Calling 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, 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—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.
CHAPTER 3

Deploy Expressway Calendar Connector with Office 365

- Hybrid Calendar Service with Office 365 Deployment Task Flow, on page 25
- Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 26
- Append the Exchange CA Certificate to the Expressway Trusted CA List, on page 28
- Link Calendar Connector to Office 365, on page 30
- Configure the Calendar Connector's Webex Site Settings, on page 31
- Start the Calendar Connector, on page 32
- Enable the Hybrid Calendar Service for Users, on page 32

Hybrid Calendar Service with Office 365 Deployment Task Flow

To deploy Hybrid Calendar Service with your Office 365 environment, perform the following tasks.

Before you begin

Prepare Your Environment, on page 1

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 26</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>
<tr>
<td>Step 2</td>
<td>(Optional) Append the Exchange CA Certificate to the Expressway Trusted CA List, on page 28</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Link Calendar Connector to Office 365, on page 30</td>
<td>Configure Exchange Servers for the Calendar Connector.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>(Optional) Configure the Calendar Connector's Webex Site Settings, on page 19</td>
<td>If you have a Cisco Webex Meetings site, configure the @Webex functionality.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Start the Calendar Connector, on page 20</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Enable the Hybrid Calendar Service for Users, on page 21</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>(Optional) Register Devices for Calendar Scheduling, on page 22</td>
<td>If you want One Button to Push (OBTP) functionality to be provided to Cisco Webex room and desk devices and Webex Boards that are registered to the Cisco Webex cloud, configure places for the devices.</td>
</tr>
<tr>
<td>Step 8</td>
<td>(Optional) Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 23</td>
<td>For OBTP on Cisco Webex room and desk devices and Webex Boards, make sure that meeting schedulers have their Personal Rooms associated with their Webex Teams accounts.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Test OBTP with Room or Desk Devices or Webex Boards, on page 24</td>
<td>If you configured OBTP in the previous step, test it with a device.</td>
</tr>
</tbody>
</table>
Register Expressway-C Connector Hosts to the Cisco Webex Cloud

Microsoft Exchange or Office 365 with Expressway Calendar Connector

• 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.

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 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 16.

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

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:
   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 Cisco Webex Hybrid Services in an Office 365 Environment**

The table lists the Certificate Authorities that your 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 (CI) 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>
<tr>
<td>Office 365 cloud</td>
<td>O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root</td>
<td>Expressway-C</td>
<td>Office 365 support</td>
</tr>
<tr>
<td>Office 365 cloud</td>
<td>O=DigiCert Inc, CN=www.digicert.com, CN=DigiCert Global Root CA, C=US</td>
<td>Expressway-C</td>
<td>Office 365 support</td>
</tr>
</tbody>
</table>
Related Topics

Supported Certificate Authorities for Cisco Spark

Link Calendar Connector to Office 365

The Calendar Connector installs automatically after you register your Expressway 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-C 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).

- **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 **Office365**.

**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 **Basic** for the **Authentication Type**.

For Hybrid Exchange (on-premises and Office 365) deployments, you can 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 presented by the Exchange Server.
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** Enter an **Email Address** so that Calendar Connector can test the connection and check that the directory query worked.

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 mailbox name, then your settings are saved without verifying connectivity.

**Step 10** Click **Add** to store the Exchange Server configuration on the Expressway-C.

The Calendar Connector tests the connection to the Exchange environment.

**Step 11** After the connector is enabled, disable and enable it again for any Exchange configuration changes to take effect.

---

**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.

---

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 19

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 21

---

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, 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.

**What to do next**

**Test the calendar features**

Follow these articles to test the Hybrid Calendar Service scheduling and out of office features with your users:

- Schedule a Cisco Webex Meeting from Your Calendar.
- Show When You're Out of Office.
Enable the Hybrid Calendar Service for Users
PART II

Hybrid Exchange and Office 365 Deployments

• Deploy Hybrid Calendar Service for a Hybrid Exchange Environment, on page 37
Deploy Hybrid Calendar Service for a Hybrid Exchange Environment

Deploy Expressway Calendar Connector for a Hybrid Exchange Environment

This chapter describes setting up the Calendar Connector on Expressway to handle both Office 365 and Microsoft Exchange in a Hybrid Exchange deployment. With the release of the cloud-based service for Office 365 users, you can now choose whether to deploy only the Expressway-based Calendar Connector, as described in this section, or a combination of the Calendar Connector and the cloud-based service.

The cloud-based service can scale beyond the 1000 user limit for Office 365 users and is simpler to deploy and maintain. It does not service Microsoft Exchange users, and currently does not support the out-of-office feature. If you deploy it alongside the Calendar Connector, your Office 365 users automatically move to the cloud-based service (unless they are in resource groups).

Before you decide which service to deploy for your Office 365 users, read the Prepare Your Environment, on page 41 chapter of the Office 365 with Cloud-Based Hybrid Calendar Service part of this guide, to understand the requirements for that option.

Before you begin

1. Prepare Your Environment, on page 1.

2. If your deployment meets all of the following criteria, you can use a simplified Exchange configuration, by following all of the steps in Deploy Expressway Calendar Connector for Microsoft Exchange, on page 11, instead of this procedure.
   
   • Your Expressway-C connects to both the on-premises Exchange environment and the Office 365 cloud through the same proxy method (either neither connects through a proxy, or both do).
   
   • Your deployment met all of the conditions for using a simplified configuration with a single impersonation account (in Set Up an Impersonation Account for Office 365, on page 4).
If your deployment does not meet these criteria, follow all of the steps in this procedure to set up two separate Exchange configurations on the Expressway-C -- one for the on-premises mailboxes, and one for the Office 365 mailboxes.

**Procedure**

**Step 1** Deploy Expressway Calendar Connector for Microsoft Exchange, on page 11 by adding an Exchange configuration to Expressway.
- You must enable and configure auto discovery when you add the configuration—Select **Use Active Directory** to enable auto discovery. We do not support manually entered Exchange addresses in Exchange hybrid environments.
- For the authentication type, you should check both **NTLM** and **Basic** authentication types. If one method fails, then the other method is used.

**Step 2** Enable Hybrid Calendar Service for users who have mailboxes in on-premises Exchange.

**Step 3** Start Calendar Connector and ensure that the activated users are subscribed.

**Step 4** As a test, in a meeting invitation in Outlook, OWA, or your calendar client, add a space scheduling keyword (such as @webex:space or @meet) to the Location field; verify that this step creates a Cisco Webex Teams space for an activated user.

**Step 5** Stop the Calendar Connector. Do not proceed until you see that it fully stopped.

**Step 6** Deploy Expressway Calendar Connector with Office 365, on page 25 by adding a new Exchange configuration to Expressway, for Office 365.

For the authentication type, you should check both **NTLM** and **Basic** authentication types. If one method fails, then the other method is used.

**Step 7** Enable Hybrid Calendar Service for users who have mailboxes in Office 365.

**Step 8** Start Calendar Connector and ensure that activated users in both on-premises and Office 365 are subscribed.

**Step 9** As a test, in an Outlook invitation, add a space scheduling keyword to the Location field; verify that this step creates a Webex Teams space for both on-premises Exchange and Office 365 users.

Users with either on-premises Exchange or Office 365 mailboxes can now schedule meetings using the scheduling keywords.

**Related Topics**

Schedule a Cisco Webex Meeting from Your Calendar
PART III

Office 365 with Cloud-Based Hybrid Calendar Service

• Prepare Your Environment, on page 41
• Deploy Cloud-Based Hybrid Calendar Service for Office 365, on page 45
Prepare Your Environment

- How the Hybrid Calendar Service Accesses User Calendars, on page 41
- Deploying Alongside an Existing Expressway-Based Calendar Connector, on page 42
- Change Processing Timeframes, on page 42
- Requirements for Hybrid Calendar Service with Microsoft Office 365, on page 43

How the Hybrid Calendar Service Accesses User Calendars

When you first set up the Hybrid Calendar Service, the setup asks you to have your organization's Office 365 tenant Global administrator account log in to the Office 365 portal to agree to allow the Hybrid Calendar Service to access Office 365 on behalf of your users.

The Hybrid Calendar Service needs these permissions to do the following actions:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read and write calendars in all mailboxes.</td>
<td>• Update the meeting text with the join details.</td>
</tr>
<tr>
<td>Sign in and read user profile.</td>
<td>• Required for the other permissions listed. The Hybrid Calendar Service does not use it directly.</td>
</tr>
<tr>
<td>Read and write all user mailbox settings.</td>
<td>• Determine the user's language for localization purposes.</td>
</tr>
<tr>
<td></td>
<td>• Read and set out-of-office status. (Feature is not available yet.)</td>
</tr>
</tbody>
</table>

When the administrator grants permission for the Hybrid Calendar Service on behalf of the Office 365 tenant, Cisco Webex is notified. This permission enables the Hybrid Calendar Service to get access tokens from Azure Active Directory (Azure AD) using OAuth 2.0, to authenticate and access user calendars. The Cisco Webex cloud does not see or store the administrator login credentials at any point in the process. For more information, see https://developer.microsoft.com/en-us/graph/docs/concepts/auth_v2_service.

The Hybrid Calendar Service uses the Microsoft Graph API to subscribe to changes in users’ calendars, receive notifications for changes made in subscribed users’ calendars, and update meeting invitations with scheduling information when the meeting location field contains keywords such as @webex or @meet, or the meeting body contains a supported video address. The Hybrid Calendar Service accesses only the calendars of the users that you enable for Hybrid Calendar Service in the Cisco Webex Control Hub.
Cisco Webex Teams follows industry-standard best practices to securely store the Private Key for the application. All meeting details that the service stores are encrypted using Webex Teams end-to-end encryption. This ensures that only those who are invited to the meeting can see the details. For more information on Webex Teams encryption, see the Cisco Webex Security and Privacy white paper.

If needed, your Exchange administrator can revoke the Hybrid Calendar Service access to your Office 365 tenant user calendars from Enterprise Applications in the Azure AD management portal.

**Deploying Alongside an Existing Expressway-Based Calendar Connector**

If you have already deployed the Expressway-based Calendar Connector to serve Microsoft Exchange users, Office 365 users or a hybrid of Microsoft Exchange and Office 365 users, you can add the cloud-based Hybrid Calendar Service with Office 365, running both at the same time. Once you enable the cloud-based service, any Office 365 users who are not a part of a resource group automatically migrate from your Calendar Connector to the new cloud-based service within 24 hours. (The Hybrid Calendar Service checks for Office 365 users to migrate from Calendar Connectors once a day.)

The Expressway-based Calendar Connector that you deploy with the Hybrid Calendar Service for Microsoft Exchange or Office 365 has a capacity limit of 1,000 Office 365 users, and requires on-premises equipment. The cloud-based service allows you to scale past the capacity limit.

- Both options (Calendar Connector and cloud-based service) can be enabled at the same time.
- All Office 365 users NOT in a resource group migrate to the cloud-based service automatically.
- To enable some users on the cloud service first for testing, put other users who must stay homed on the on-premises Connector into a resource group before turning on the cloud-based service.

**Change Processing Timeframes**

When you activate the Hybrid Calendar Service for Office 365 and enable users or move mailboxes, the service processes these changes periodically.

*Table 3: Processing Frequency for Activations and Changes*

<table>
<thead>
<tr>
<th>Administrator Action</th>
<th>Processing Behavior</th>
<th>Expected Completion Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable the Hybrid Calendar Service for the organization.</td>
<td>Once the setup is successful, the Hybrid Calendar Service tries to subscribe to calendars of users that are listed in &quot;Not activated&quot; or &quot;Error&quot; states.</td>
<td>Depending on volume, immediate to minutes.</td>
</tr>
<tr>
<td>Administrator Action</td>
<td>Processing Behavior</td>
<td>Expected Completion Timeframe</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Enable individual users (toggle on Calendar or bulk enable).</td>
<td>Hybrid Calendar Service attempts to subscribe to the user's calendar. If the activation fails, the user is in &quot;Error&quot; state and the Hybrid Calendar Service retries in 60 minutes. If the activation fails multiple times, the Hybrid Calendar Service retries in 24 hours.</td>
<td>If everything goes well, immediately. Otherwise, up to 24 hours. If it takes longer than this, check the user account.</td>
</tr>
<tr>
<td><strong>Mailbox Migration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move user mailbox from on-premises Exchange to Office 365.</td>
<td>Once Office 365 has completed the mailbox migration, it takes up to 40 minutes for the Hybrid Calendar Service to put the user in &quot;Error&quot; state. As above, the Hybrid Calendar Service attempts to reprocess users in &quot;Error&quot; state every 60 minutes.</td>
<td>If everything goes well, up to 100 minutes. Otherwise, up to 24 hours. If it takes longer than this, check the user account.</td>
</tr>
<tr>
<td>Move user mailbox from Office 365 to on-premises Exchange.</td>
<td>Once a day, the Hybrid Calendar Service runs a watch refresh that detects missing mailboxes and puts them in &quot;Error&quot; state. Another cloud service then reassigns the user to an Expressway-based Calendar Connector.</td>
<td>Up to 24 hours to detect the change, plus a few minutes of reassignment time.</td>
</tr>
</tbody>
</table>

**Requirements for Hybrid Calendar Service with Microsoft Office 365**

- An Office 365 tenant with Exchange Online accounts for users in the organization. During setup, you must be able to sign in as a Global administrator for the tenant to grant application permissions.

Note the following considerations for your Office 365 tenant:

- We currently only support a single Office 365 tenant per Cisco Webex organization.

- We only support the Worldwide instance of Office 365. (Other instances which we do not support include USGovDoD, USGovGCCHigh, China and Germany.)

- Although your tenant may use Multi-Geo Capabilities in Office 365 to store data in a chosen geography, Cisco Webex Teams stores data only in U.S. data centers. (For more details, see section 3 of the Cisco Webex Service Privacy Data Sheet.)
• For @webex scheduling, any supported Cisco Webex Meetings release.
  You must enable the Personal Room feature for the Webex site and for the individual users.

• A Cisco Webex organization with a paid subscription.

• Each Cisco Webex hybrid calendar user must be assigned a paid license that provides access to core
  Cisco Webex messaging and meeting services.

• Users must have activated Cisco Webex accounts, with email addresses that are exact matches in Cisco
  Webex Meetings, Webex Teams, and Exchange Online (the Primary Email Address).

Each Webex Teams user can only have one email address associated with only one Hybrid Calendar
Service integration. In other words, the Hybrid Calendar Service will only process meetings from a single
address for creating spaces, decorating meetings, showing the meetings list and join button, and sending
One Button to Push (OTBP) to video devices.
CHAPTER 6

Deploy Cloud-Based Hybrid Calendar Service for Office 365

- Hybrid Calendar Service with Office 365 Deployment Task Flow, on page 45
- Prepare Your Cisco Webex Meetings Site, on page 46
- Enable and Configure Hybrid Calendar Service with Office 365, on page 46
- Enable the Hybrid Calendar Service with Office 365 for Users, on page 47
- Register Devices for Calendar Scheduling, on page 48
- Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 49
- Test the Office 365 and Hybrid Calendar Service Integration, on page 50
- Move a User from an Expressway-Based Connector, on page 50

Hybrid Calendar Service with Office 365 Deployment Task Flow

To deploy Hybrid Calendar Service with your Office 365 organization, perform the following tasks.

Before you begin
Prepare Your Environment, on page 41

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Prepare Your Cisco Webex Meetings Site, on page 46</td>
<td>If you have a Cisco Webex Meetings site, make sure it's ready for integration with @webex.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable and Configure Hybrid Calendar Service with Office 365, on page 46</td>
<td>Register your Office 365 environment to the Cisco Webex cloud, test the connection, and set the default Webex site.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable the Hybrid Calendar Service with Office 365 for Users, on page 47</td>
<td>If you want One Button to Push (OBTP) functionality to be provided to cloud-registered room and desk devices and Webex Boards, configure places for the devices.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Register Devices for Calendar Scheduling, on page 48</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Have Users Associate Their Webex Personal Rooms with Cisco Webex Teams, on page 49</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Test the Office 365 and Hybrid Calendar Service Integration, on page 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Move a User from an Expressway-Based Connector, on page 50</td>
<td></td>
</tr>
</tbody>
</table>

---

**Prepare Your Cisco Webex Meetings Site**

In order to provide full @webex functionality, the Hybrid Calendar Service needs access to user scheduling information from your Cisco Webex Meetings site.

If your Webex site is managed in Cisco Webex Control Hub, you do not need to do anything to make the information available. Otherwise, the preferred method for making this information available is to have an administrator link the site to Webex Teams.

If you have not yet linked the sites, your users can associate their Cisco Webex Personal Rooms with Cisco Webex Teams themselves in the app.

**Enable and Configure Hybrid Calendar Service with Office 365**

Follow these steps to register your Office 365 environment to the Cisco Webex cloud, test the connection, and set the default Webex site. The setup wizard in https://admin.webex.com guides you through the process.

**Before you begin**

- You should either be the Global administrator for the Office 365 tenant or have the administrator with you when you begin the setup process.

**Procedure**

**Step 1**
From https://admin.webex.com, go to Services.

**Step 2**
On the hybrid calendar card with the Office 365 logo, click Set Up.

**Step 3**
Follow the steps to authorize Cisco Webex cloud access on your Office 365 Global administrator account. The browser should redirect you to https://admin.webex.com when you've finished the authorization steps. If it does not, try these steps again.

**Step 4**
In the Hybrid Calendar setup window, enter the email address of an account in Office 365 to test the connection, and click Test.

The Hybrid Calendar Service tests by creating an event in the user's calendar to validate access and provisioning.

**Step 5**
When the setup finishes, click Done.

**Step 6**
On the hybrid calendar card with the Office 365 logo, click Edit settings.
Step 7
Choose or type the Cisco Webex Meetings site to use for @webex scheduling. Save your changes.

Step 8
If there are users with error status, click User Status Report to view the error details.

Enable the Hybrid Calendar Service with Office 365 for Users

Use this procedure to enable individual Cisco Webex users for Hybrid Calendar Service with Office 365. See the links below for ways to enable services for your Cisco Webex users in bulk or in a directory synchronized organization.

Any of these methods requires that users have signed in to the 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
- Users must have licensed Exchange Online mailboxes.
- Users must have activated Cisco Webex accounts, with email addresses that are exact matches in Cisco Webex Meetings, Webex Teams, and Exchange Online (the Primary Email Address).

Procedure

Step 1
From the customer view in https://admin.webex.com, go to Users, and then choose a specific user from the list.

You can use the search function to narrow down the list of users.

Step 2
Click the row to open an overview of the user.

Step 3
In the Hybrid Services area, click Calendar Service.

Step 4
Toggle on Calendar, ensure that Microsoft Exchange/Office 365 is selected, and save your changes.

After you activate the service, the user's calendar service status changes to Pending Activation and then 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.

Related Topics
- Disable User Email Notifications
- Steps to update users in bulk
- Steps to update users in a directory synchronized organization
Register Devices for Calendar Scheduling

Use this procedure to prepare cloud-registered Cisco Webex room and desk devices and Webex Boards for One Button to Push (OBTP). Repeat the procedure for each device that users will include in meeting invitations. Each device must have its own unique calendar mailbox.

Before you begin

Cisco Webex Calling:

• After you add a Cisco Webex Calling 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, 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—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 the Office 365 and Hybrid Calendar Service Integration

Use these steps to set up a test meeting and verify the Office 365 integration. Direct users to the documentation below for how to schedule meetings.

Procedure

Step 1  
Sign into Outlook, Outlook Web Access, or https://mail.office365.com with one of the test Office 365 user accounts enabled for Hybrid Calendar Service.

Step 2  
Test the team space scheduling keyword (such as @webex:space or @meet):

a)  
Create a new meeting, and then add the keyword to the Location field. To create a new Webex team space for the meeting, invite at least two other people.

b)  
To test One Button to Push on a video device, 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 then click Save.

d)  
Open https://teams.webex.com, and sign in with the test user account.

e)  
Verify whether a new space was created (if you added two or more other invitees) and contains the calendar invite card. If you only invited one other invitee, the calendar invite card will appear in the conversation space between your test account and the invitee.

f)  
Verify that the meeting invitation is updated with the details to join the meeting with Webex Teams.

g)  
If you're testing One Button to Push on a video device, when the meeting is scheduled to begin, verify that the Join button appears on the device.

Step 3  
Test the Personal Room scheduling keyword (such as @webex):

a)  
Create a new meeting, and then add the keyword to the Location field.

b)  
To test One Button to Push on a video device, 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 then click Save.

d)  
Verify that the meeting invitation is updated with the details to join the meeting.

e)  
If you're testing One Button to Push on a video device, when the meeting is scheduled to begin, verify that the Join button appears on the device.

Related Topics

Schedule a Cisco Webex Meeting from Your Calendar

Move a User from an Expressway-Based Connector

The Hybrid Calendar Service automatically moves any Office 365 users who are not part of a resource group from your Expressway-based Calendar Connector to the cloud-based service. This process can take up to an hour, because the service checks for users to move once an hour. (If you're also moving the user's mailbox
from Microsoft Exchange to Office 365, it can take up to 40 minutes longer.) If you want to have users activated faster, use the following procedure to toggle the Hybrid Calendar Service for users, thereby forcing the activation within minutes.

**Procedure**

**Step 1**
If applicable, move the user mailbox from Microsoft Exchange to Office 365.

**Step 2**
From the customer view in https://admin.webex.com, go to **Users**.

**Step 3**
To modify an individual user, do the following sub-steps:

a) Search for the user in the list and click the row for that user.

b) In the panel that opens on the right, click **Calendar Service**.

c) From the Resource Group drop-down list, click **None**.

d) Next to **Calendar**, toggle the service off.

e) Wait a minute, and then toggle the service back on.

The user should be activated within a few minutes.

**Step 4**
To modify users in bulk, do the following sub-steps:

a) Click **Manage Users**, and choose **CSV Add or Modify User**.

b) Click **Export** to download the file.

c) Edit the exported_users.csv file.

d) For any users that you want to move, delete the value in the Hybrid Calendar Service Resource Group column.

e) Save a first copy of the file in this state, for use later.

f) To speed the move, set Hybrid Calendar Service (Exchange) to **FALSE**.

g) Save a second copy of the file.

h) Click **Import**, select the second file copy that you saved, and click **Open**.

i) Choose **Add and remove services**, and click **Submit**.

   If you also add new users in this process and don't suppress admin invite emails, new users receive activation emails.

j) Wait several minutes, and then re-import the first copy of the file.

   The users should be activated within a few minutes.

---

**Note**

You must remove Office 365 users from a resource group in order for them to move off of the Calendar Connector. This procedure also covers that process.
PART IV

Google Calendar

• Prepare Your Environment, on page 55
• Deploy Hybrid Calendar with Google Calendar, on page 57
CHAPTER 7

Prepare Your Environment

- Requirements for Hybrid Calendar Service With Google Calendar, on page 55
- Remove Google Hangouts Information in Meeting Events, on page 55

Requirements for Hybrid Calendar Service With Google Calendar

- A Cisco Webex organization with one of the offers documented for the Hybrid Calendar Service in License Requirements for Cisco Webex Hybrid Services.
- A Google G Suite organization (formerly Google Apps for Work) with the following accounts:
  - Google accounts for all users in the organization (each user's Google account email address must match their Cisco Webex Teams login address)
  - Optionally, an access control list (ACL) account if you use meeting room resources
- For @webex, a Cisco Webex Meetings site:
  - You must enable the Personal Room feature for the Webex site and for the individual users.
  - The Google account email address should also match the user's Webex account address. If it does not, users must associate their Webex Personal Room with Webex Teams in the app in order to use @webex.

Note

Each Webex Teams user can only have one email address associated with only one Hybrid Calendar Service integration. In other words, the Hybrid Calendar Service will only process meetings from a single address for creating spaces, decorating meetings, showing the meetings list and join button, and sending One Button to Push (OTBP) to video devices.

Remove Google Hangouts Information in Meeting Events

In your G Suite Calendar settings, consider removing the video calls that are automatically added to events. This step ensures that meeting events contain just Cisco Webex join links when your users send them out. These steps do not disable Google Hangouts.
## Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From <a href="https://admin.google.com">https://admin.google.com</a>, go to Apps &gt; G Suite &gt; Calendar.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Sharing settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Under Video Calls, uncheck <em>Automatically add video calls to events created by a user.</em></td>
</tr>
</tbody>
</table>
Deploy Hybrid Calendar with Google Calendar

Enable and Configure Hybrid Calendar Service with Google Calendar

Follow these steps to register your Google Calendar environment to the Cisco Webex cloud, enable API access, test the connection, and set the default Webex site. The setup wizard in https://admin.webex.com guides you through the process.

Procedure

**Step 1**
From https://admin.webex.com go to Services, and then choose one:
- For a new environment, click Set Up on the hybrid calendar card. Choose the Google logo, and then click Next.
- If you have an existing Exchange environment registered for Hybrid Calendar Service and want to add Google Calendar, click Set Up under the Google section of the card, and then click Next.

**Step 2**
Follow the steps to authorize Cisco Webex cloud access on your G Suite account. You need to copy information from https://admin.webex.com, so keep it open in a browser tab.
- Click the link to open https://admin.google.com, and then go to ➔ Security > Show more > Advanced settings
- In the Authentication section, click Manage API client access.
- Enter or copy-paste the Client Name and One or More API Scopes, as provided on https://admin.webex.com.
- Click Authorize.
- Return to https://admin.webex.com, and then click Next.

**Step 3**
Fill out account information for a test G Suite account. This is used to test the connection with Google Calendar.
Enable the Hybrid Calendar Service with Google for Users

Use this procedure to enable a small number of Cisco Webex users for Hybrid Calendar Service with Google Calendar.

See Ways to Add and Manage Users in Cisco Webex Control Hub for other methods, such as using a bulk CSV template.

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.)

Procedure

Step 1 From the customer view in https://admin.webex.com, go to Users, and then choose a specific user from the list.

You can use the search function to narrow down the list of users.

Step 2 Click the row to open an overview of the user.

Step 3 Choose one and then save your changes:

- In a new environment, click Calendar Service, toggle on Calendar, and ensure that the Google Calendar is selected.
- In an existing environment with Exchange, click Calendar Service, and under calendar type, ensure that the Google Calendar is selected.
After you activate the service, the Cisco Webex 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.

**What to do next**

Test the calendar features

*Schedule a Cisco Webex Meeting from Your Calendar.*

### Register Devices for Calendar Scheduling

**Before you begin**

**Cisco WebexCalling:**

- After you add a Cisco Webex Calling 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**—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 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 the Google Calendar And Hybrid Calendar Service Integration

Use these steps to set up a test meeting and verify the Google Calendar integration. Direct users to the documentation below for how to schedule meetings.

Procedure

Step 1 Sign in to https://calendar.google.com with one of the test Google user accounts enabled for Hybrid Calendar Service.
Step 2 Click Create to start an event, and then add a space scheduling keyword (such as @webex:space or @meet) to the Where field. Fill out other meeting information, as needed, and then click Save.
Step 3 Open https://teams.webex.com, and sign in with the test user account.
Step 4 Verify whether a new Cisco Webex space was created and contains the calendar invite card.
Step 5 To test One Button to Push (OBTP) with a Cisco Webex room or desk device or Webex Board:
   a) In https://calendar.google.com, click Create to start an event, and then add a scheduling keyword (such as @webex) to the Location field.
   b) Click Rooms, and choose the device you want to add.
   c) Fill out other meeting information, as needed, and then click Save.
   d) When the meeting is scheduled to begin, verify that the Join button appears on the device.

Related Topics
- Schedule a Cisco Webex Meeting from Your Calendar
Test the Google Calendar and Hybrid Calendar Service Integration
Known Issues with Hybrid Calendar Service

- Exchange and Office 365 (Expressway-Based Calendar Connector), on page 63
- Office 365 (Cloud-Based Service), on page 65
- Google Calendar (Cloud-Based Service), on page 67

Exchange and Office 365 (Expressway-Based Calendar Connector)

Calendar Connector Deployment and Configuration

- A top priority issue—fixed in Calendar Connector version 8.8-1.0.5158—causes two problems configuring the Calendar Connector on Expressway X8.11:

1. Entering an email address in the Discovery section of the Microsoft Exchange Configuration page causes the configuration to fail. On Calendar Connector versions earlier than 8.8-1.0.5158, the only way to configure a new Calendar Connector or change the Exchange configuration with X8.11 is by leaving the Email Address field blank, which means that you will not be able to test your configuration as you save it. As a workaround, use the steps in Test Microsoft Exchange Autodiscovery and Impersonation to try to simulate the test, from a machine that has network conditions as similar as possible to the Expressway-C.

2. On the Webex Configuration page, using the Test Connection button causes the same failure. The workaround is to click Save without testing.

Note

Make sure you're running Calendar Connector version 8.8-1.0.5158 or later before upgrading to X8.11 on any Expressway-C hosting the Calendar Connector.

- Calendar Connector supports single cluster with a maximum of two Expressway instances per organization.
- Proxy connections must use basic authentication or no username and password. No other authentication schemes are supported.
- The Calendar Connector currently does not support Exchange organizations that require the service (impersonation) account to use multi-factor authentication (MFA).
• For some customers, the Calendar Connector raises a critical alarm described as "Redirected Microsoft Exchange Autodiscovery URL not trusted." The issue may result in some delays processing calendar events for users. In some cases, the Calendar Connector will be unable to provide any service to some portion of the users.

If you see this alarm, use the Autodiscover Redirect URL trust list to configure how the Calendar Connector can locate user mailboxes.

• For some customers, the Calendar Connector raises an "NTLM authentication error: Credentials cannot be used for NTLM authentication" warning in the hybrid_services_log files. This can occur if a connector proxy is configured on the Applications > Hybrid Services > Connector Proxy page in Expressway and that proxy requires authentication. No workaround is required as long as the connector proxy supports Basic authentication scheme, or does not require authentication.

• If you deregister the Calendar Connector, or deactivate it if it's the only hybrid service on the Expressway, the Expressway can get into an error state where hybrid service connectors will not register, configuration changes do not propagate, or other problems occur. The workaround is to reboot the Expressway and reregister the connector.

• You cannot search in https://admin.webex.com to return the set of users who have hybrid calendar service turned on or off.

General Scheduling Issues (All Keywords)

• If you add a scheduling keyword or supported video address to a single instance of a recurring meeting series, the meeting join details are not updated. As a workaround, add the keyword or video address to the entire meeting series.

• Users may see multiple meeting invitations in their Outlook inbox when receiving meetings scheduled with a keyword or supported video address. As a workaround, check the following checkboxes in the Microsoft Outlook Web app under Settings > Calendar > Automatic Processing:
  • Delete meeting requests and responses that have been updated
  • Automatically process requests and responses from external senders

These settings are available only in the web app, but the above changes apply to all Outlook clients.

• Hybrid Calendar Service does not add meeting join links to the meeting invitation for any invitees who have single quotes around their email addresses. As a workaround, do not include single quotes around email addresses in the invitation.

• In some versions of Microsoft Outlook 2016, after changing a single instance of a recurrent scheduled meeting where a scheduling keyword is in the location field, the body text and join links might disappear.
  • If possible, upgrade to the latest version of Outlook.
  • If you cannot upgrade, delete and reschedule the affected instance.
  • The other instances of the meeting series should be unaffected.

• Meeting organizers using Microsoft Outlook 2011 for Mac may not see the join links in their meeting invites, although the invitees receive the links. This is an issue with Outlook 2011 for Mac and the solution is to upgrade to a more recent version of Outlook for Mac.
• Hybrid Calendar Service does not automatically add meeting join information to a meeting that's scheduled in the past.

**Scheduling a Webex Personal Room Meeting (Keywords Including @webex, @meet:myroom)**

• Hybrid Calendar Service does not add Webex details if the meeting invitation already contains Webex join links (for example, added with Productivity Tools or manually by the meeting organizer). The meeting organizer can manually delete any previously added join links so that Hybrid Calendar Service can add the new join links.

**Scheduling in a Cisco Webex Teams Space (Keywords Including @webex:space, @meet, @spark)**

• Space keyword scheduling currently supports a maximum of 75 meeting participants. A meeting organizer who invites more than 75 participants will receive an email message indicating that they have exceeded the maximum.

• Space keyword scheduling does not currently handle distribution lists. Individual members of the distribution list still receive the meeting invitation with details on joining the space, but are not automatically added to the space. As a workaround, the meeting organizer can expand the mailer on the TO line before sending the invite. That way, each user is individually added to the space.

• Attachments that users add to meeting invites with space keywords are not added to the corresponding space.

**One Button to Push (OBTP)**

• For issues involving the Join button and meetings list in the Webex Teams app, see the applicable Meetings section for each type of client in the Cisco Webex Teams Known Issues article.

---

**Office 365 (Cloud-Based Service)**

**Deployment**

• Office 365 users who are assigned to the cloud-based service (indicated in Cisco Webex Control Hub as on cluster "Cisco Webex Cloud") may show a persistent error message in Control Hub, "Could not find cluster with Calendar Connector. Select another Resource Group, or configure a new cluster with Calendar Connector." This error can be ignored.

**Feature Parity with the Expressway-Based Calendar Connector**

• The out-of-office status feature is not yet available. This feature is currently only available with Exchange and Office 365 integrations that use the Expressway-based Calendar Connector.

If you use the Calendar Connector and add the new cloud-based Hybrid Calendar Service for Microsoft Office 365, any Office 365 users who are not in a resource group will automatically migrate from the Connector to the cloud-based service. Make sure that these users know they will lose this functionality until it is implemented in the cloud-based service. If out-of-office status is important to your users, consider waiting to deploy the new cloud-based service until the feature is available.
• The cloud-based Hybrid Calendar Service for Microsoft Office 365 uses the Language setting from the scheduler's Region and time zone settings (Options > General > Region and time zone setting in Outlook) to determine which language to use when adding join details to a meeting. It does not allow you to set a default language for the entire organization as the Calendar Connector does. (For more information, see How the Hybrid Calendar Service Localizes Meeting Details.)

General Scheduling Issues (All Keywords)

• If you add a scheduling keyword or supported video address to a single instance of a recurring meeting series, the meeting join details are not updated. As a workaround, add the keyword or video address to the entire meeting series.

• Hybrid Calendar Service does not automatically add meeting join information to a meeting that's scheduled in the past.

Scheduling a Webex Personal Room Meeting (Keywords Including @webex, @meet:myroom)

• Hybrid Calendar Service does not add Webex details if the meeting invitation already contains Webex join links (for example, added with Productivity Tools or manually by the meeting organizer). The meeting organizer can manually delete any previously added join links so that Hybrid Calendar Service can add the new join links.

Scheduling in a Cisco Webex Teams Space (Keywords Including @webex:space, @meet, @spark)

• Space keyword scheduling currently supports a maximum of 75 meeting participants. A meeting organizer who invites more than 75 participants will receive an email message indicating that they have exceeded the maximum.

• Space keyword scheduling does not currently handle distribution lists. Individual members of the distribution list still receive the meeting invitation with details on joining the space, but are not automatically added to the space. As a workaround, the meeting organizer can expand the mailer on the TO line before sending the invite. That way, each user is individually added to the space.

• Attachments that users add to meeting invites with space keywords are not added to the corresponding space.

• If you use a space keyword on a meeting invitation that includes just one invitee, and that invitee is not already a Cisco Webex Teams user, no space is created for the meeting, the invitation is not updated with join details, and the user is not invited to use Webex Teams.

One Button to Push (OBTP)

• For issues involving the Join button and meetings list in the Webex Teams app, see the applicable Meetings section for each type of client in the Cisco Webex Teams Known Issues article.
Google Calendar (Cloud-Based Service)

General Scheduling Issues (All Keywords)

• If you add a scheduling keyword or supported video address to a single instance of a recurring meeting series, the meeting join details are not updated. As a workaround, add the keyword or video address to the entire meeting series.

• Hybrid Calendar Service does not automatically add meeting join information to a meeting that's scheduled in the past.

Scheduling a Webex Personal Room Meeting (Keywords Including @webex, @meet:myroom)

• Hybrid Calendar Service does not add Webex details if the meeting invitation already contains Webex join links (for example, added with Productivity Tools or manually by the meeting organizer). The meeting organizer can manually delete any previously added join links so that Hybrid Calendar Service can add the new join links.

Scheduling in a Cisco Webex Teams Space (Keywords Including @webex:space, @meet, @spark)

• Space keyword scheduling currently supports a maximum of 75 meeting participants. A meeting organizer who invites more than 75 participants will receive an email message indicating that they have exceeded the maximum.

• Space keyword scheduling does not currently handle distribution lists. Individual members of the distribution list still receive the meeting invitation with details on joining the space, but are not automatically added to the space. As a workaround, the meeting organizer can expand the mailer on the TO line before sending the invite. That way, each user is individually added to the space.

• Attachments that users add to meeting invites with space keywords are not added to the corresponding space.

• If you use a space keyword on a meeting invitation that includes just one invitee, and that invitee is not already a Cisco Webex Teams user, no space is created for the meeting, the invitation is not updated with join details, and the user is not invited to use Webex Teams.

One Button to Push (OBTP)

• For a meeting scheduled with a space keyword between two people and with an associated room or desk device, the One Button to Push (OBTP) join button does not show up on the device. The invite is treated as a one-on-one call and not a joinable meeting.

• For issues involving the Join button and meetings list in the Webex Teams app, see the applicable Meetings section for each type of client in the Cisco Webex Teams Known Issues article.
Google Calendar (Cloud-Based Service)
Troubleshoot Hybrid Calendar Service

- Diagnostic Tools on Expressway-C Connector Host, on page 69
- Check Connector Health on Expressway-C, on page 69
- Roll Back to the Previous Version of a Connector, on page 70

Diagnostic Tools on Expressway-C Connector Host

Use these diagnostic tools to investigate a problem with Cisco Webex Hybrid Services connectors installed on the Expressway-C.

- Access the Hybrid Services log levels and enable debug mode if instructed to do so by support. Go to Maintenance > Diagnostics > Hybrid Services Log Levels.
- Check the event log for errors and warnings. Go to Status > Logs > Event Log.
- Check for related alarms on Status > Alarms. Alarms related to Cisco Webex Hybrid Services are tagged [Hybrid Services] and have IDs in the 60000–69999 range. You can also see these alarms in Cisco Webex Control Hub (https://admin.webex.com).
- Run diagnostic logging while you recreate the issue, and take a tcpdump during that period. Go to Maintenance > Diagnostics > Diagnostic logging and read the online help for more details.
- Take a system snapshot to provide support for diagnosis. Go to Maintenance > Diagnostics > System snapshot.
- Configure syslog if you have remote logging servers. Go to Maintenance > Logging.
- Configure incident reporting so that any Expressway failures are automatically reported to us. Go to Maintenance > Diagnostics > Incident reporting > Configuration.

For more details, read the Cisco Expressway Serviceability Guide, or search the help on the Expressway.

Related Topics
Send Hybrid Service Expressway Connector Logs to the Cloud

Check Connector Health on Expressway-C

When you're having a problem with Cisco Webex Hybrid Services, you can check the status of the connectors and restart any stopped connectors.
Before you begin
If a connector is stopped, we recommend that you open a ticket with support and send a log first before you restart the connector.

Procedure

Step 1
On the Expressway-C, go to Applications > Hybrid Services > Connector Management to check the status of your connectors.

The Connector Management section shows all the installed connectors, their version numbers and their status.

Step 2
If a connector is Stopped, click the name of that connector.

You'll see a more detailed status page with a Restart button.

Step 3
Click Restart.

What to do next
If the restart generates an alarm, or if the connector stops again, try the following:

• Follow the guidance on the alarm. You can also see these alarms in Cisco Webex Control Hub (https://admin.webex.com).
• From the customer view in https://admin.webex.com, click your username, and then click Feedback to open a ticket and send logs.
• Use the diagnostic tools to look for problem signatures.
• Roll back to the previous version of the connector (try this if the problem started after a connector upgrade).

Related Topics
Send Expressway Connector Logs
Contact Support

Roll Back to the Previous Version of a Connector

Under normal conditions, your Expressway-C upgrades your connectors automatically after you choose to upgrade in Cisco Webex Control Hub or set a scheduled upgrade time. You can roll back to the previous version of a connector if something goes wrong with an upgraded connector.

Procedure

Step 1
On the Expressway-C, go to Applications > Hybrid Services > Connector Management to check the health status of your connectors.
The Connector Management section shows all the installed connectors, their version numbers, and their status.

**Step 2**

Click the name of the connector.

A more detailed status page shows the currently installed version and the version that you can roll back to. The page also shows any versions that you previously rejected (by rolling back from them).

**Step 3**

Click Roll back to reject the currently installed version, and replace it with the Target version.

The page displays the formerly installed version number in the Rejected version field, which means that the will not allow that version to install itself in future.

If you click Back to connector list, you can see the previous version is now running. An alarm is raised because you rejected an upgrade. You can safely ignore that alarm; it appears because of your choice, and it is lowered when a newer version is installed.

When a newer version is available on Cisco Webex, the automatic upgrade resumes.

**Step 4**

To reverse your decision and accept the Rejected version, click Allow this upgrade.
Important Items for Hybrid Services Deployments

This section provides added context about key configuration items that relate to Cisco Webex Hybrid Services. These points are crucial if you want to successfully deploy Expressway-hosted Cisco Webex Hybrid Services, such as Hybrid Call Service Aware/Connect and Hybrid Calendar Service. We've highlighted these items in particular for the following reasons:

- We want to explain them, so that you understand their role in a hybrid deployment and feel reassured.
- They are mandatory prerequisites that ensure a secure deployment between our cloud and your on-premises environment.
- They should be treated as pre-day zero activities: they can take a bit longer to complete than typical configuration in a user interface, so allow a timeframe to get these items sorted.
- After these items are addressed in your environment, the rest of your Cisco Webex Hybrid Services configuration will go smoothly.

Supported Certificate Authorities

The Expressway-C connector host must be registered to Cisco Webex in order for hybrid services to work. Expressway-C is deployed in the internal network, and the way it registers to the cloud is through an outbound HTTPS connection—the same type that is used for any browser that connects to a web server.

Registration and communication to the Cisco Webex cloud uses TLS. Expressway-C is the TLS client, and the Cisco Webex cloud is the TLS server. As such, Expressway-C checks the server certificate.

The certificate authority signs a server certificate using its own private key. Anyone with the public key can decode that signature and prove that the same certificate authority signed that certificate.

If Expressway-C has to validate the certificate provided by the cloud, it must use the public key of the certificate authority that signed that certificate to decode the signature. A public key is contained in the certificate of the
certificate authority. To establish trust with the certificate authorities used by the cloud, the list of certificates of these trusted certificate authorities must be in the Expressway's trust store. Doing so, the Expressway can verify that the call is truly coming from the Cisco Webex cloud.

With manual upload, you can upload all relevant certificate authority certificates to the trust store of Expressway-C.

With automatic upload, the cloud itself uploads those certificates in the trust store of Expressway-C. We recommend that you use automatic upload. The certificate list might change, and automatic upload guarantees that you get the most updated list.

If you allow automatic installation of certificate authority certificates, you are redirected to https://admin.webex.com (the management portal). The redirection is done by the Expressway-C itself without any user intervention. You, as the Cisco Webex administrator, must authenticate through an HTTPS connection. Soon after, the cloud pushes the CA certificates to the Expressway-C.

Until the certificates are uploaded to the Expressway-C trust store, the HTTPS connection cannot be established. To avoid this problem, the Expressway-C is preinstalled with Cisco Webex-trusted CA certificates. Those certificates are only used to set up and validate the initial HTTPS connection, and they don't appear in Expressway-C trust list. Once the certificates of the trusted certificate authorities are pulled from the cloud through this initial HTTPS connection, those certificates are available for platform-wide usage; then, they appear in the Expressway-C trust list.

This process is secure for these reasons:

- Requires admin access to Expressway-C and to https://admin.webex.com. Those connections use HTTPS and are encrypted.
- Certificates are pushed from the cloud to Expressway using the same encrypted connection.

This list shows the certificate authority certificates that the Cisco Webex cloud currently uses. This list might change in the future:

- C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
- C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certificate Authority
- C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2
- C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certificate Authority

A list of certificate authority certificates is also required for the Expressway-E in the traversal pair. Expressway-E communicates with the Cisco Webex cloud using SIP with TLS, enforced by mutual authentication. Expressway-E trusts calls coming from and going to the cloud, only if the CN or SAN of the certificate presented by the cloud during TLS connection setup matches the subject name configured for the DNS zone on Expressway ("Unified CM"). The certificate authority releases a certificate only after an identity check. The ownership of the Unified CM domain must be proved to get a certificate signed. Because we (Cisco) own that domain, the DNS name "Unified CM" is direct proof that the remote peer is truly Cisco Webex.
Exchange Impersonation Account

Calendar Connector integrates Cisco Webex with Microsoft Exchange 2010, 2013, 2016, or Office 365 through an impersonation account. The application impersonation management role in Exchange enables applications to impersonate users in an organization to perform tasks on behalf of the user. The application impersonation role must be configured in Exchange and is used in the Calendar Connector as part of the Exchange configuration on the Expressway-C interface.

The Exchange impersonation account is Microsoft's recommended method for this task. Expressway-C administrators don't need to know the password, because the value can be entered in the Expressway-C interface by an Exchange administrator. The password isn't clearly shown, even if the Expressway-C administrator has root access to the Expressway-C box. The password is stored encrypted using the same credential encryption mechanism as other passwords on the Expressway-C.

For additional security, follow the steps in Deploy Expressway Calendar Connector for Microsoft Exchange, on page 11 to enable TLS in order to secure EWS connections on the wire.