Prepare your environment

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 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 Webex cloud. You can allow the Webex cloud to upload CA certificates to the Expressway-C trust store. Or, in the case where security policies prevent the Webex cloud from uploading trusted certificate authority certificates on Expressway-C, you may upload them manually.

Calendar connector

The calendar connectoris the on-premises component of the Hybrid Calendar. The connector runs on an Expressway-C host that you register to the 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 Webex App spaces and Webex personal rooms.

The Hybrid Calendar 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 updates per user per hour
- The size of calendars

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

Calendar connector or cloud-based 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. 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).

The cloud-based service supports the TelePresence Management Suite (TMS) scheduling option. This integration allows the service to leverage your on-premises resource management and conference hosting environment for simplified meeting scheduling. The integration also extends the meeting join experience to a wide range of video devices. The cloud-based service links to the on-premises TMS by using the calendar connector. For this reason, you cannot deploy the TMS integration in the same organization with a calendar connector that is configured for Microsoft Exchange or Office 365.

Before you decide which service to deploy for your Office 365 users, read the Prepare your environment chapter of the Office 365 with cloud-based Hybrid Calendar part of this guide, to understand the requirements for that option.

Requirements for Hybrid Calendar

Product	Release
Webex App	Hybrid Calendar is available with the offers documented in License Requirements for Webex Hybrid Services.
Expressway—download from software.cisco.com at no charge	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.
Microsoft Exchange	• 2013, 2016, 2019 • Microsoft 365
Webex Meetings—Use for @webex scheduling only; not required for scheduling meetings in Webex team spaces.	Any supported Webex Meetings release You must enable the Personal Room feature for the Webex site and for the individual users.

Each user's email address in the calendar system (Microsoft Exchange or Microsoft 365) must match their Webex App login address. To use @webex, the address should also match the user's 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 App user can only have one email address associated with only one Hybrid Calendar integration. In other words, the Hybrid Calendar will only process meetings from a single address for creating spaces, decorating meetings, showing the meetings list and join button, and sending the **Join** button to video devices.

Set Up an impersonation account for on-premises Microsoft Exchange

The Microsoft Exchange impersonation account (https://msdn.microsoft.com/en-us/library/office/dn722377(v=exchg.150).aspx) is a key integration point for the Hybrid Calendar. The service uses the impersonation account for continuous authentication with Microsoft Active Directory domain controllers and Microsoft Exchange Client Access Servers.

To ensure that impersonation remains secure and continuously connected, we recommend an account maintenance strategy such as using two impersonation accounts. This can prevent exposure to password expiry, which could take the service offline. To periodically rotate between the accounts, you change the account in the Calendar Connector configuration. The example in the following table shows one possible account rotation scheme, though you may choose a different strategy to ensure security and connectivity based on your organization's requirements:

Date	Account A hybridcalendarA@example.com	Account B hybridcalendarB@example.com
January 1	Set password	Set password

Date	Account A hybridcalendarA@example.com	Account B hybridcalendarB@example.com
January 8	Configure Calendar Connector with account A	—
March 1	—	Change password
March 8	—	Update Calendar Connector with account B
May 1	Change password	—
May 8	Update Calendar Connector with account A	—
July 1	—	Change password
July 8	—	Update Calendar Connector with account B
Repeat the password rotation and Calendar Connector update process with both accounts.		

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 Unity Connection, 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 the Microsoft Docs ApplicationImpersonation role article.

Procedure

Step 1 Sign in to a server on which Exchange Management Shell is installed. Sign in with one of the following accounts:

- An account that is a member of the Enterprise Admins group.
- An account that can grant permissions on Exchange objects in the configuration container.

Step 2 Run the following command in Exchange Management Shell:

new-ManagementRoleAssignment -Name:`RoleName` -Role:ApplicationImpersonation -User '`ServiceUserName`'

where:

- **`RoleName`** is the name that you want to give the assignment, for example, **`CalendarConnectorAcct`**. The name that you enter for **`RoleName`** appears when you run **get-ManagementRoleAssignment**.
- **`ServiceUserName`** is the name of the account you selected, in domain\alias format.

Related Topics

Exchange Impersonation Account

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 Unity Connection, 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

Complete the prerequisites for Hybrid Calendar

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, 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 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 *.ciscospark.com, *.rackcdn.com, *.wbx2.com, *.webex.com, and *.webexcontent.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 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 TMS 15.0 and 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.

- 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 and Productivity Tools plugin for meeting invitations:
  - Hybrid Calendar (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 plan to deploy a hybrid Exchange environment with Office 365, you must enable TNEF for remote domains in Exchange Online. Having TNEF disabled causes Exchange Online to strip the TMS:ExternalConferenceData and UCCapabilities attributes, breaking OBTP for Unified CM-registered endpoints. For more information on TNEF, see https://docs.microsoft.com/en-us/exchange/mail-flow/content-conversion/tnef-conversion.

If you have on-premises conferencing, you can add OBTP with 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 Hybrid Services

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

Before you begin

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

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 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 (Exchange or Office 365) on a dedicated Expressway-C:
  - calendar connector can be hosted on multiple Expressway-C clusters of up to 6 nodes each.
  - 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.

Hybrid Calendar is highly available if Exchange and Expressways are deployed in a cluster. The same guidelines apply for the Expressway-C connector host clustering. For more information, see User Capacity Limits for Expressway-Based Hybrid Services.

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 Webex cloud. **Do not change the MAC address of the Expressway virtual machine when using VMware tools, or you risk losing service.**

- You do not require a release key, or an Expressway series key, to use the virtual Expressway-C for Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
- Use the Expressway web interface in a supported browser. (See the Cisco Expressway Administrator Guide.) The interface may or may not work in unsupported browsers. You must enable JavaScript and cookies to use the Expressway web interface.

Step 5 If this is your first time running Expressway, you get a first-time setup wizard to help you configure it for Hybrid Services.

Select **Webex Hybrid Services**. This ensures that you will not require a release key.

Step 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)

Note Expressway-C connector hosts do not support dual NIC deployments.

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:
  - Enable H.323 protocol. On **Configuration** > **Protocols** > **H.323** page, set **H.323 Mode** to On.

    H.323 mode is required for clustering, even if the Expressway does not process H.323 calls.

    Note You may not see the **H.323** menu item if you used the Service Select wizard to configure the Expressway for Hybrid Services. You can work around this problem by signing in to the Expressway console and issuing the command `xconfig H323 Mode: "On"`.

  - **System** > **Clustering** > **Cluster name** should be an FQDN.

    Typically this FQDN is mapped by an SRV record in DNS that resolves to A/AAAA records for the cluster peers.

  - **System** > **Clustering** > **Configuration primary** should be 1.
  - **System** > **Clustering** > **TLS verification mode** should be Permissive, at least until you add a second peer.

    Select Enforce if you want cluster peers to validate each others' certificates before allowing intercluster communications.

  - **System** > **Clustering** > **Cluster IP version** should match the type of IP address of this Expressway-C.
  - **System** > **Clustering** > **Peer 1 address** should be the IP address or FQDN of this Expressway

    Each peer FQDN must match that Expressway's certificate if you are enforcing TLS verification.

Caution To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.

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

- All traffic between Expressway-C and the Webex cloud is HTTPS or secure web sockets.

- TCP port 443 must be open outbound from the Expressway-C. See https://collaborationhelp.cisco.com/article/WBX000028782 for details of the cloud domains that are requested by the Expressway-C.

Step 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** .

Note The details of the proxy, as configured on the primary Expressway in the connector host cluster, are shared throughout the Expressway cluster. You cannot configure different proxies for different nodes in the cluster.

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

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

  You can let Webex manage the root CA certificates for you. However, if you choose to manage them yourself, be aware of certificate authorities and trust chains; you must also be authorized to make changes to the Expressway-C trust list.

- 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.