

# Configure Webex Connect Email App with Office365 Oauth

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Step 1: Start email app configuration on Webex Connect](#)

[Step 2: Create an app in Microsoft Azure](#)

[Step 3: Configure mailbox user on Office365](#)

[Step 4: Configure Email App on Webex Connect](#)

[Verify](#)

[Troubleshooting](#)

## Introduction

This document describes the steps to configure an Email app for Office365 with Open Authorization (OAuth 2.0).

Contributed by Andrius Suchanka and Bhushan Suresh, Cisco TAC Engineer.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Webex Contact Center (WxCC) 2.0
- Webex connectportal with Email flows configured
- MS Azure access
- MS Office365 access

### Components Used

The information in this document is based on these software versions:

- WxCC 2.0
- Cisco Webex Connect
- Microsoft Azure
- Microsoft Office365

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

### Step 1: Start email app configuration on Webex Connect

Start Email app configuration on Webex Connect platform.

-Login to your Webex Connect tenant;

-Navigate to 'Assets->Apps', click 'Configure New App' and select 'Email'. Select 'OAuth 2.0' for authentication type, copy and store 'Forwarding Address' and 'Call Back URL' for later configuration steps:

< Configure New Application - Email

Enter the mail server settings for your account to start sending and receiving emails using Webex Connect.

Asset Name <sup>ⓘ</sup>

Asset Name

Register To Webex Engage  Configure Outbound Webhooks  DOCS <sup>🔗</sup>

Email ID

Email ID

Forwarding Address

b6b9072db2ce25198b45f08c9a9e

Note: Emails sent to the asset email ID will be forwarded to this address.

Authentication Type

OAuth 2.0

SMTP Server

Username

Port

Security

None

Client ID

Client Secret

Call Back URL

https://[redacted].us.webexconnect.io/callback

Proceed to configuration on Microsoft side.

### Step 2: Create an app in Microsoft Azure

Register an app in Azure portal as per '[Register an application with the Microsoft identity platform](#)' document.

-Login to <https://portal.azure.com>;

-Navigate to 'Azure Active Directory', select 'App registrations' and click 'New registration';

-Provide application name, select appropriate account type, input Web 'Redirect URI' with your tenant name (that is <https://yourwebexconnectname.us.webexconnect.io/callback> as seen in step 1) and register the app:

# Register an application ...

## \* Name

The user-facing display name for this application (this can be changed later).

 ✓

## Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Cisco Systems, Inc only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

## Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

  ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) [↗](#)

**Register**

-After app is registred - navigate to 'Authentication', scroll down to 'Implicit grand and hybrid flows', select 'Access tokens' option and save:

Search

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding & properties
  - Authentication**
  - Certificates & secrets
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

### Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Cisco Systems, Inc only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

**⚠** Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

### Advanced settings

#### Allow public client flows

Enable the following mobile and desktop flows:

Yes **No**

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

#### App instance property lock

Save Discard

-Navigate to 'Certificates & secrets', select 'Client Secrets', click 'New client secret', add a description and validity length:

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | Certificates & secrets

Overview  
Quickstart  
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

**+ New client secret**

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

### Add a client secret

Description:

Expires:

**Add** **Cancel**

-Copy client secret value and store it for later use:

All services > Cisco Systems, Inc | App registrations > WebexConnect

### WebexConnect | Certificates & secrets

Search  Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
wxconnect	10/26/2024	L1e8Q~B5rzySjA6wI3PqgNqZkdVd1zpTJ...	5f7981e4-9b3e-43ff-b2cf-297606955fff

-Navigate to 'API permissions', click 'Add a permission', select 'APIs my organization uses', in search field input 'office 365' and select 'Office 365 Exchange Online'. Select 'Application permissions', expand 'Mail' section, check 'Mail.Send' and click 'Add permission':

All services > Cisco Systems, Inc | App registrations > WebexConnect

### WebexConnect | API permissions

Search  Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. The

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for Cisco Systems, Inc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

#### Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Name

- Office 365 Enterprise Insights
- Office 365 Exchange Online**
- Office 365 Information Protection
- Office 365 Management APIs
- Office 365 SharePoint Online

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest
- Support + Troubleshooting
- Troubleshooting
- New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. The

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cisco Systems, Inc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

**Request API permissions**

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
Other permissions	
<input type="checkbox"/> full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	
Exchange	
IMAP	
Mailbox	
MailboxSettings	
Mail (1)	
<input type="checkbox"/> Mail.Read Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadWrite Read and write mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.Send Send mail as any user	Yes
Organization	

[Add permissions](#) [Discard](#)

-After said permission is added, admin consent has to be granted. Click on 'Grant admin consent':

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest
- Support + Troubleshooting
- Troubleshooting
- New support request

**Grant admin consent confirmation.**

Do you want to grant consent for the requested permissions for all accounts in Cisco Systems, Inc? This will update any existing admin consent records this application already

[Yes](#) [No](#)

Configured permissions



Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cisco Systems, Inc





API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	
Office 365 Exchange Online (1)				
Mail.Send	Application	Send mail as any user	Yes	⚠ Not granted for Cisco S...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

-Navigate to 'Overview' and note down 'Application (client) ID' and 'Directory (tenant) ID' for further configuration use:

 Delete  Endpoints  Preview features

 Overview

-  Quickstart
-  Integration assistant
- Manage**
-  Branding & properties
-  Authentication

^ Essentials



Display name : [WebexConnect](#)  
Application (client) ID : 56ba9bac-67be-4bd2-b551-47258e7ead62  
Object ID : 3d6317c3-ed51-4ff2-955d-019ac1637beb  
Directory (tenant) ID : 0f47778c-61c2-4b0a-8e94-3f05e737a1dd  
Supported account types : [My organization only](#)

Note: make sure that that user consent for apps is allowed in Azure under 'Consent and permissions' for 'Enterprise applications' (this is a default settings):

[Home](#) > [Enterprise applications | Consent and permissions](#) >

 Consent and permissions | User consent settings ...

«  Save  Discard |  Got feedback?

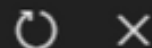
- Manage**
-  User consent settings
-  Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.


- User consent for applications  
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)
- Do not allow user consent  
An administrator will be required for all apps.
  - Allow user consent for apps from verified publishers, for selected permissions (Recommended)  
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
  - Allow user consent for apps  
All users can consent for any app to access the organization's data.

### Step 3: Configure mailbox user on Office365

- Login to <https://admin.microsoft.com>;
- Navigate to Users->Active Users;
- Select a user with a mailbox for integration with Webex Connect;
- After selecting specific user navigate to 'Mail', under 'Email apps' click on 'Manage email apps', make sure that 'Authenticated SMTP' is selected and click 'Save changes':



**John**

 [Reset password](#)

[Change photo](#)

[Account](#)

[Devices](#)

[Licenses and apps](#)

**[Mail](#)**

[OneDrive](#)

**Mailbox storage**

0.01% (5.791MB/50GB)

[Learn more about mailbox storage quotas](#)

### Mailbox permissions

[Read and manage permissions \(0\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

### Show in global address list

Yes

[Manage global address list visibility](#)

### Automatic replies

Off

[Manage automatic replies](#)

### Email apps

All apps allowed

**[Manage email apps](#)**

### Email forwarding

Applied

[Manage email forwarding](#)

### More actions

[Edit Exchange properties](#)





# Manage email apps

Choose the apps where John can access Microsoft 365 email.


- Outlook on the web
- Outlook desktop (MAPI)
- Exchange web services
- Mobile (Exchange ActiveSync)
- IMAP
- Pop
- Authenticated SMTP

Save changes

-Under 'Email Forwarding' click on 'Manage email forwarding', select 'Forward all emails sent to this mailbox', fill in 'Forwarding email address' with alias from Webex Connect App configuration as seen in step 1 (additionally if needed select 'Keep a copy of forwarded email in this mailbox') and click 'Save changes':



**John**

 [Reset password](#)

[Change photo](#)

[Account](#)

[Devices](#)

[Licenses and apps](#)

**[Mail](#)**

[OneDrive](#)

**Mailbox storage**

0.01% (5.791MB/50GB)

[Learn more about mailbox storage quotas](#)

**Mailbox permissions**

[Read and manage permissions \(0\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

**Show in global address list**

Yes

[Manage global address list visibility](#)

**Automatic replies**

Off

[Manage automatic replies](#)

**Email apps**

All apps allowed

[Manage email apps](#)

**Email forwarding**

Applied

**[Manage email forwarding](#)**

**More actions**

[Edit Exchange properties](#)



# Manage email forwarding

Forward all emails sent to this mailbox

The mailbox owner will be able to view and change these forwarding settings.

Forwarding email address \*

a41a0ba3566ed2091155f13e48e6d4f8@mail-us.imiconnect.io

Keep a copy of forwarded email in this mailbox

Save changes

-Make sure that outbound email forwarding to external email addresses is allowed in your Microsoft 365 Defender portal.

