

Configure Webex Connect Email Asset with Open Authorization

Contents

[Introduction](#)

[Reason to use OAuth 2.0](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Step 1: Create a Project on Google Developer Console](#)

[Step 2: Configure OAuth Consent](#)

[Step 4. Create OAuth Credentials](#)

Introduction

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

Contributed by Anuj Bhatia and Bhushan Suresh, Cisco TAC Engineer.

Reason to use OAuth 2.0

Google has deprecated the **Less secure app access** feature and this requires configuration of the Email Asset with OAuth 2.0 for Authentication for use with Third-party Apps, such as Webex connect.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Webex Contact Center (WxCC) 2.0
- Webex connect portal with Email flows configured

Components Used

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

- WxCC 2.0

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.

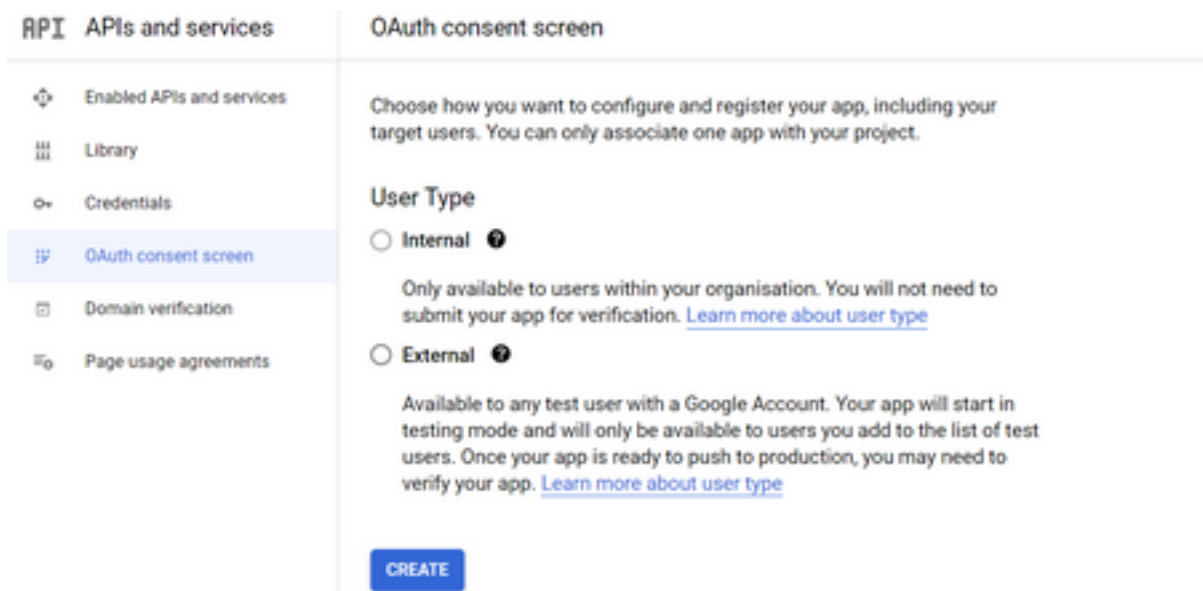
Configure

Step 1: Create a Project on Google Developer Console

Please follow the steps to create a [Google project](#)

Step 2: Configure OAuth Consent

1. Choose `Internal` or `External` as required.



The screenshot shows the 'OAuth consent screen' configuration page in the Google Developer Console. On the left, there is a navigation menu under 'APIs and services' with options: 'Enabled APIs and services', 'Library', 'Credentials', 'OAuth consent screen' (highlighted), 'Domain verification', and 'Page usage agreements'. The main content area is titled 'OAuth consent screen' and contains the following text: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Below this is the 'User Type' section with two radio button options: 'Internal' and 'External'. The 'Internal' option is selected. Below the 'Internal' option, there is explanatory text: 'Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)'. Below the 'External' option, there is explanatory text: 'Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)'. At the bottom of the main content area, there is a blue 'CREATE' button.

2. Click Create.

3. Enter the **User Support Email** which is the Email ID associated on the Asset.

// On the Asset:

ASSET NAME ⓘ
bhusuresIMIEmail

EMAIL ID
bhusuresimi@gmail.com

FORWARDING ADDRESS
5fcf6cf5e57fb5d9410efd884845ed66@mai [COPY](#)

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

// On the Google Console:

Google Cloud Platform IMIOAuth

API APIs & Services

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen**
- Domain verification
- Page usage agreements

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
IMIOauth
The name of the app asking for consent

User support email *
bhusuresimi@gmail.com
For users to contact you with questions about their consent

App logo [BROWSE](#)
Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

Note: Please make sure you are logged in with the Email ID associated with the Asset or the **User Support Email** does not show the the email in the drop-down list.

Google Cloud Platform IMIOAuth Search Products, resources, docs (/)

APIs & Services Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

App information
This shows in the consent screen, and helps end users know who you are and contact you

App name *
IMIOAuth
The name of the app asking for consent

User support email *
bhuresimi@gmail.com
For users to contact you with questions about their consent

Learn

This account is managed by google.com. Learn more

bhushan imi
bhuresimi@gmail.com
Privacy
Google Account

How is this...
This is the...
G Sign in with Google

[Display Name] can access

Add account Sign out

Select what [Display Name] can access

4. Enter the Authorized Domain as the Webex connect domain as shown:

Authorized domains ?

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

Authorized domain 1 *
imiconnect.io

+ ADD DOMAIN

5. Enter Save and Continue and under Test users enter the same user email as the **User Support Email**.

Edit app registration

✓ OAuth consent screen — ✓ Scopes — 3 **Test users** — 4 Summary

Test users

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

+ ADD USERS

Filter Enter property name or value ?

User information	
bhusuresimi@gmail.com	

SAVE AND CONTINUE CANCEL

6. Enter Save and Continue and go **Back to the Dashboard**.

Step 4. Create OAuth Credentials

1. Navigate to Credentials > Create credentials and select **OAuth client ID**.

The screenshot shows the Google Cloud console interface. On the left, the 'APIs and services' sidebar is visible, with 'Credentials' highlighted. A red arrow points from the 'Credentials' link in the sidebar to the 'Create Credentials' button in the main content area. The 'Create Credentials' dropdown menu is open, showing several options: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. The 'OAuth client ID' option is highlighted with a red box, and another red arrow points to it from the right. Below the dropdown, the 'API keys' and 'OAuth 2.0 Client IDs' sections are visible, both showing 'No API keys to display' and 'No OAuth clients to display' respectively.

2. Create and enter the details:

Application Type: **Web Application**

Authorized JavaScript origins: **WebEx Connect URL**

Authorized redirect URIs: The callback URL (This URL can be found on the Email Asset page once Authentication Type as OAuth 2.0 is chosen.)

Google Cloud Platform IMIOAuth

API APIs & Services

← Create OAuth client ID

Enabled APIs & services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
Web client 2

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ

For use with requests from a browser

URIs 1 *
https://webexccwithwxcaspbx.imiconnect.io

+ ADD URI

Authorized redirect URIs ⓘ

For use with requests from a web server

URIs 1 *
https://webexccwithwxcaspbx.imiconnect.io/callback

+ ADD URI

Note: It may take 5 minutes to a few hours for settings to take effect

CREATE CANCEL

<1

3. Copy the **Client ID**, **Client Secret**, and Download the JSON.

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services



OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Your Client ID

[Redacted Client ID] 

Your Client Secret

[Redacted Client Secret] 





DOWNLOAD JSON



OK

4. On Webex Connect, create an Asset (Under Asset > Apps > Configure New Application > Email) and enter the details:

ASSET NAME 

REGISTER TO WEBEX CC [DOCS](#) 

Registered on 2022-03-10 23:02:29.0 and assigned to bhuresa_IMI_New_Integration

EMAIL ID

FORWARDING ADDRESS

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

AUTHENTICATION TYPE

SMTP SERVER USERNAME

PORT SECURITY

CLIENT ID CLIENT SECRET

CALL BACK URL

AUTHORIZATION URL

SCOPE

ACCESS TOKEN URL

REFRESH TOKEN URL

5. Click Generate Token and you are redirect to the Gmail log in.

EMAIL ID

FORWARDING ADDRESS

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

AUTHENTICATION TYPE

SMTP SERVER

PORT

CLIENT ID

CALL BACK URL

AUTHORIZATION URL

SCOPE

ACCESS TOKEN URL

REFRESH TOKEN URL

