

Configuración de Webex Connect Email Asset con autorización abierta

Contenido

[Introducción](#)

[Motivo para utilizar OAuth 2.0](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Paso 1: Crear un proyecto en Google Developer Console](#)

[Paso 2: Configurar el consentimiento de OAuth](#)

[Paso 4. Creación de Credenciales de OAuth](#)

Introducción

Este documento describe los pasos para configurar un recurso de correo electrónico con autorización abierta (OAuth 2.0).

Colaboración de Anuj Bhatia y Bhushan Suresh, ingeniero del TAC de Cisco.

Motivo para utilizar OAuth 2.0

Google ha dejado de utilizar la función de **acceso a aplicaciones menos seguras** y esto requiere la configuración del recurso de correo electrónico con OAuth 2.0 para la autenticación para su uso con aplicaciones de terceros, como Webex connect.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de contacto Webex (WxCC) 2.0
- Portal de conexión de Webex con flujos de correo electrónico configurados

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

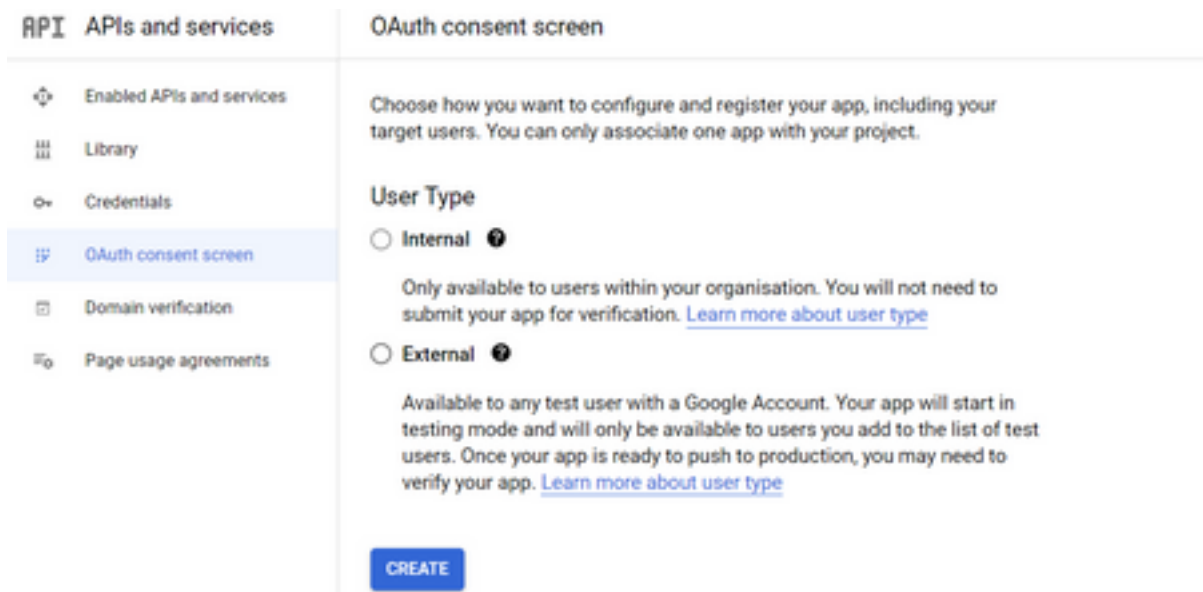
Configurar

Paso 1: Crear un proyecto en Google Developer Console

Siga los pasos para crear un [proyecto de Google](#)

Paso 2: Configurar el consentimiento de OAuth

1. Seleccione Internal External según sea necesario.



The screenshot shows the 'APIs and services' section of the Google Developer Console. The 'OAuth consent screen' option is selected in the left-hand navigation menu. 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 is the 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 is the 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 page is a blue 'CREATE' button.

2. Haga clic en Create.

3. Introduzca el **correo electrónico de asistencia al usuario**, que es la ID de correo electrónico asociada al activo.

// En el recurso:

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.

// En la consola de Google:

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.

Nota: Asegúrese de que ha iniciado sesión con la ID de correo electrónico asociada al recurso o de que el mensaje de **correo electrónico de asistencia al usuario** no muestra el correo electrónico en la lista desplegable.

4. Introduzca el dominio autorizado como dominio de conexión Webex, como se muestra:

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 *

[+ ADD DOMAIN](#)

5. ingrese Save and Continue y en Test users introduzca el mismo correo electrónico de usuario que el correo electrónico de asistencia al usuario.

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	
bhuresimi@gmail.com	

SAVE AND CONTINUE CANCEL

6. ingrese Save and Continue y vaya a Volver al panel.

Paso 4. Creación de Credenciales de OAuth

1. Acceda a Credentials > Create credentials y seleccione OAuth client ID.

API APIs and services

Credentials + CREATE CREDENTIALS DELETE

Enabled APIs and services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Create credentials to access your API

Remember to

API keys

Name

No API keys to display

OAuth 2.0 Client IDs

Name

No OAuth clients to display

API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so that your app can access the user's data.

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

2. Cree e introduzca los detalles:

Tipo de aplicación: **Aplicación web**

Orígenes de JavaScript autorizados: **URL de WebEx Connect**

URI de redirección autorizados: La URL de devolución de llamada (esta URL se puede encontrar en la página de recursos de correo electrónico una vez que se ha seleccionado el tipo de autenticación como OAuth 2.0).

Google Cloud Platform IMIOAuth

RPI 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://webexcccwithwxcaspbx.imiconnect.io

+ ADD URI

Authorized redirect URIs

For use with requests from a web server

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

+ ADD URI

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

CREATE CANCEL

3. Copie el ID de cliente, **Secreto de cliente** y 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. En Webex Connect, cree un recurso (en Asset > Apps > Configure New Application > Email) e introduzca los detalles:

ASSET NAME  bhusuresIMIEmail

REGISTER TO WEBEX CC [CONFIGURE OUTBOUND WEBHOOKS](#) [DOCS](#)

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

EMAIL ID bhusuresimi@gmail.com

FORWARDING ADDRESS [COPY](#)

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

AUTHENTICATION TYPE OAuth 2.0

SMTP SERVER smtp.gmail.com USERNAME bhusuresimi@gmail.com

PORT 487 SECURITY SSL

CLIENT ID CLIENT SECRET

CALL BACK URL <https://webexccwithwxcaspbx.imiconnect.io/callback>

AUTHORIZATION URL <https://accounts.google.com/o/oauth2/auth>

SCOPE <https://mail.google.com/>

ACCESS TOKEN URL <https://oauth2.googleapis.com/token>

REFRESH TOKEN URL <https://oauth2.googleapis.com/token>

[GENERATE TOKEN](#)

5. Haga clic en Generate Token y se le redirigirá al inicio de sesión de Gmail.

EMAIL ID bhusuresimi@gmail.com

FORWARDING ADDRESS 5fc6cf5e57fb5d9410efd884845ed66@mail [COPY](#)

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

AUTHENTICATION TYPE OAuth 2.0

SMTP SERVER smtp.gmail.com

PORT 587

CLIENT ID

CALL BACK URL <https://webexccwithwxcaspbx.imiconnect.io/callback>

AUTHORIZATION URL <https://accounts.google.com/o/oauth2/auth>

SCOPE <https://mail.google.com/>

ACCESS TOKEN URL <https://oauth2.googleapis.com/token>

REFRESH TOKEN URL <https://oauth2.googleapis.com/token>

[GENERATE TOKEN](#)

