

# Configurar o ativo de e-mail do Webex Connect com autorização aberta

## Contents

[Introduction](#)

[Motivo para usar OAuth 2.0](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Passo 1: Criar um projeto no Console do desenvolvedor do Google](#)

[Etapa 2: Configurar o Consentimento OAuth](#)

[Etapa 4. Criar Credenciais OAuth](#)

## Introduction

Este documento descreve as etapas para configurar um ativo de e-mail com autorização aberta (OAuth 2.0).

Contribuição de Anuj Bhatia e Bhushan Suresh, engenheiro do Cisco TAC.

## Motivo para usar OAuth 2.0

O Google substituiu o recurso **Acesso de aplicativo menos seguro** e isso requer a configuração do Ativo de e-mail com OAuth 2.0 para autenticação para uso com aplicativos de terceiros, como Webex connect.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Webex Contact Center (WxCC) 2.0
- Portal do Webex connect com fluxos de e-mail configurados

## Componentes Utilizados

As informações neste documento são baseadas nestas versões 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

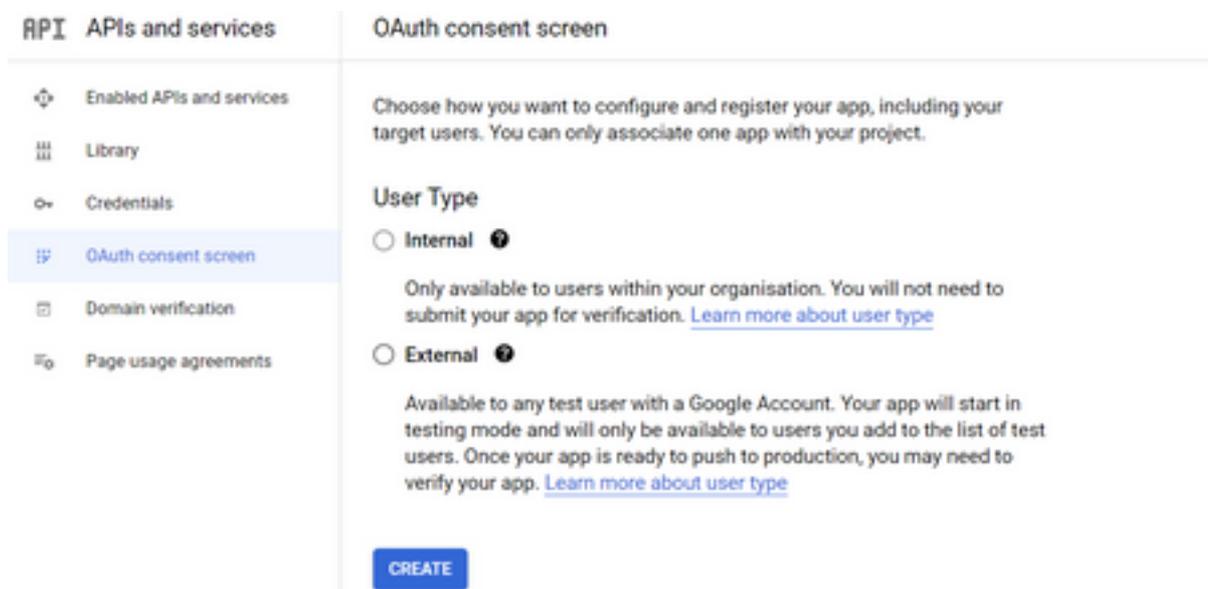
## Configurar

### Passo 1: Criar um projeto no Console do desenvolvedor do Google

Siga as etapas para criar um [projeto do Google](#)

### Etapa 2: Configurar Consentimento OAuth

1. Escolha `Internal` ou `External` conforme necessário.



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. Clique em `Create`.

3. Insira o **E-mail de suporte do usuário**, que é a ID do e-mail associada no ativo.

// No ativo:

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.

// No 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:** Verifique se você está conectado com a ID de e-mail associada ao ativo ou se o e-mail de suporte ao usuário não mostra o e-mail na lista suspensa.

4. Insira o Domínio Autorizado como o domínio de conexão do Webex conforme mostrado:

### 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. Enter Save and Continue e sob Test users digite o mesmo e-mail do usuário que o e-mail de suporte do usuário.

## 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. Enter Save and Continue e vá Voltar ao Painel.

## Etapa 4. Criar Credenciais OAuth

1. Navegue até Credentials > Create credentials e selecione ID do cliente OAuth.

API APIs and services

Enabled APIs and services

Library

**Credentials**

OAuth consent screen

Domain verification

Page usage agreements

Credentials + CREATE CREDENTIALS DELETE

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. Crie e informe os detalhes:

Tipo de aplicativo: **Aplicativo Web**

Origens de JavaScript autorizadas: **URL do WebEx Connect**

URIs de redirecionamento autorizados: A URL de retorno de chamada (essa URL pode ser encontrada na página Email Asset (Ativo de email) depois que Authentication Type (Tipo de autenticação) como OAuth 2.0 for escolhido.)

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://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 a ID do Cliente, o Segredo do Cliente e 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. No Webex Connect, crie um ativo (em Asset > Apps > Configure New Application > Email) e insira os detalhes:

ASSET NAME 

REGISTER TO WEBEX CC  [DOCS](#) 

Registered on 2022-03-10 23:02:29.0 and assigned to bhuresi\_MI\_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. Clique em Generate Token e você será redirecionado para o login do Gmail.

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

